Use of Facial Recognition Technology for Medical Purposes: Balancing Privacy with Innovation

Seema Mohapatra*

Abstract

Imagine applying for a job, and as part of your application process, your prospective employer asks for a photograph. You, as an eager candidate, comply with the request and, unbeknownst to you, the employer runs your picture through a software program that scans you for any common genetic diseases and that estimates your longevity. Alas, your face indicates that you may die young. No job for you.

Although this sounds like science fiction, we may not be that far off from this scenario. In June 2014, scientists from Oxford reported that they have developed a facial recognition program that uses ordinary family photos to help diagnose rare genetic conditions. Part II of this Article describes the potential applications of facial recognition technology in medicine that have recently been explored, highlighting the recent software that may be used for genetic screening. Part III delves into the heightened need for privacy when dealing with genetic conditions and discusses an individual's right not to know about their genetic predispositions. Part IV discusses the history of facial recognition technology in the United States and how it has been monitored and regulated. This Part concludes that the current and proposed regulatory regime for facial recognition technology is not well suited for medical applications of such technology. Part V examines whether health-related legislation, such as the Health Insurance Portability and Accountability Act of

* Associate Professor of Law, Dwayne O. Andreas School of Law, Barry University, Orlando, Florida. B.A., Johns Hopkins University, 1995; J.D., Northwestern University School of Law, 2000; M.P.H., Yale University, 1997. Sincere thanks to Elizabeth Pendo, Kelly Dineen, Michael Morley, and to the participants of the University of St. Louis School of Law Faculty Workshop and Barry University School of Law Faculty Workshop for helpful comments about this Article. Much gratitude to Dean Leticia Diaz for summer research grant support and to Kati Haupt for her invaluable research assistance.

1996 (HIPPA), the Genetic Information Nondiscrimination Act (GINA), the Food, Drug, and Cosmetic Act (FDCA), or the American with Disabilities Act (ADA), provides adequate privacy protection from software that uses facial recognition to screen for diseases or health and concludes that they do not. Finally, Part VI outlines what kinds of restrictions are needed on the use of this technology to protect patient's privacy. Such restrictions could be located within GINA or ADA or could be part of a comprehensive regulation on facial recognition technology in general. Whichever form it takes, such protections are needed to ensure that what could be a very helpful technology is not used to discriminate against individuals or to reveal information to a person who may not seek such knowledge.

TABLE OF CONTENTS

I. INTRODUCTION

Imagine applying for a job, and as part of your application process, your prospective employer asks for your photograph. You, as an eager candidate, comply with the request, and, unbeknownst to you, the employer runs your picture through a software program that scans you for any common genetic diseases and that estimates your longevity. Alas, your face indicates that you may die young and have an increased likelihood of having Marfan's syndrome, which is associated with fatal aortic aneurysms. Other candidates do not have these risk factors, and you are denied the job.

Although this sounds like science fiction, we may not be that far off from this scenario. In the summer of 2014, Oxford scientists reported that they have developed a facial recognition program that uses ordinary family photos to help diagnose rare genetic conditions.[1] Under current law, it may not be long before such software is commercially available for general use, including use by employers.

Part II of this Article describes this and other potential applications of facial recognition technology in medicine that have recently been explored, highlighting the recent software that may be used for genetic screening and

1. Chris Weller, *Rare Genetic Disorders Could Be Diagnosed with Facial Recognition Computer Software*, MED. DAILY (June 24, 2014, 3:04 PM), http://www.medicaldaily.com/rare-genetic-disorders-could-be-diagnosed-facial-recognition-computer-software-289688.

predicting longevity. This Part also explores potential ways these applications may be used. The next Part delves into the heightened need for privacy when dealing with health status, especially genetic conditions, and discusses an individual's right not to know about their genetic predispositions. Part IV discusses the ways that facial recognition technology is being regulated in the United States. This Part concludes that the current and proposed regulatory regime for facial recognition technology is not well suited for medical applications of such technology. Part V examines whether health-related legislation, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA),[2] the Genetic Information Nondiscrimination Act (GINA),[3] the Food Drug and Cosmetic Act (FDCA),[4] or the Americans with Disabilities Act (ADA),[5] provides adequate privacy protection from software that uses facial recognition to screen for diseases or health and concludes that they do not. Finally, Part VI outlines what kinds of restrictions are needed on the use of this technology to protect patients' privacy.

This Article does not argue that the development of facial recognition technology for medical purposes should be curbed. Such use could be very revolutionary and beneficial for certain patients. However, there needs to be a restriction on the use of such technology so that the resulting information cannot be used by others, such as employers, for discriminatory purposes. Restrictions could be located within GINA or ADA regulations or could be part of a comprehensive regulation on facial recognition technology in general. Whichever form it takes, such protections are needed to ensure that what could be a very helpful technology is not used to discriminate against individuals or to reveal information to a person who may not seek such knowledge.

II. MEDICAL AND HEALTH APPLICATIONS OF FACIAL RECOGNITION TECHNOLOGY

Facial recognition technology (FRT) refers to systems and computer programs that analyze images for identification purposes.[6] When one thinks of

2. 29 U.S.C. § 1181 (2012).
3. 42 U.S.C. § 2000ff (2012).
4. 21 U.S.C. § 301 (2012).
5. 42 U.S.C. § 12101.
6. *Q&A on Face-Recognition*, ACLU, https://www.aclu.org/technology-and-liberty/qa-face-recognition (last visited Mar. 14, 2016). The programs utilize measurements of facial characteristics to create a unique file called a "template." *Id.* The FRT software compares the template to stored images

FRT, one usually thinks of it being used for security or surveillance purposes. Currently, FRT is used mainly for verification or authentication, which matches a face-print with an individual record to identify a person.[7] This application is very useful for law enforcement to identify suspects.[8] Another common use is for identifying an unknown person from an anonymous picture.[9] Current commercial uses of FRT include, but are not limited to, general surveillance, police initiatives (such as predicting what a missing child may look like several years later), business-targeted marketing efforts, and social media application.[10] Medical applications of FRT have not been commonly used but that may soon change.[11]

---

and formulates a score that estimates the similarities. *Id.*

7. *Id.*

8. *See, e.g.*, Ben Sobel, *Facial Recognition Technology Is Everywhere. It May Not Be Legal*, WASH. POST (June 11, 2015), https://www.washingtonpost.com/news/the-switch/wp/2015/06/11/facial-recognition-technology-is-everywhere-it-may-not-be-legal/.

9. *Q&A on Face-Recognition*, *supra* note 6.

10. *See generally* Jonathan Shaw, *FACEbook Confidential: The Privacy Implications of Facebook's Surreptitious and Exploitative Utilization of Facial Recognition Technology*, 31 TEMP. J. SCI. TECH. & ENVTL. L. 149, 149–50 (2012).

There has been much discussion of the Facebook FRT fiasco. "FRT is a major contributor to the spectre of an Orwellian society. Facebook uses it to identify 'friends' from uploaded photos, which are permanently affixed in cyberspace and accessible to the government." Kimberly N. Brown, *Anonymity, Faceprints, and the Constitution*, 21 GEO. MASON L. REV. 409, 409 (2014).

"Facebook's 'tag suggestion' function automatically retrieves the names of individuals in photos uploaded by its one billion users at a rate of three hundred million a day." *Id.* at 431. "Using only Facebook and commercially available FRT, researchers in 2012 were able to identify college students more than 30 percent of the time, retrieving their names, photos, and other personal information from Facebook—including the first five digits of social security numbers—with the privacy settings turned on." *Id.* at 429.

A concern raised about social media, and Facebook in particular, is that although Facebook stated that the data stored is monitored, restricted, encrypted, and secured, its privacy policy still holds the right to "access, preserve and share information when we have a good faith belief it is necessary to: detect, prevent and address . . . illegal activity" or "to protect ourselves, you and others." *Id.* Government systems employing FRT have access to social networking sites and can use the data to identify people. *Id.* at 431. It was further revealed that the NSA has a program that can directly access data through companies such as Facebook "for purposes of obtaining search histories, email content, file transfers, and live chats." *Id.* at 432.

11. John Lynn, *A Biometrically Controlled Healthcare System*, EMR, EHR & HIPPA (Sept. 6, 2013), http://www.emrandhipaa.com/tag/facial-recognition/. Lynn dreams about a future with an "ID-free" doctor's office that could potentially recognize a patient's face and ensure his or her records were readily available for the physician. *Id.*

A. FRT and Genetic Conditions

In June 2014, researchers from Oxford reported that they had developed computer software that uses facial feature recognition to look for similarities from a bank of computer-based photos of facial structures that have similar genetic conditions, such as Down syndrome.[12] At the time of the report, the software correctly predicted a genetic disorder, on average, ninety-three percent of the time.[13]

The concept of using facial feature recognition to diagnose diseases is not new because many rare disorders do not have an accompanying genetic test and specialists rely on analysis of facial features to help in diagnosis.[14] However, doctors with the requisite skill set for such diagnoses are scarce. There are over 17,000 genetic disorders that have been diagnosed, of which about 700 can be diagnosed with the assistance of abnormal facial characteristic recognition.[15] The program developed by the scientists at Oxford currently can help identify ninety individual disorders, and the hope is that it will be used where specialists are unavailable.[16] The software is not currently used as a sole test for diagnosis but is used for assisting pediatricians in the process.[17] In the future, this program could be used to identify those born with a detectable disorder, allowing for the option of early treatment.[18] According to the study, previous work has established that thirty to forty percent of all rare genetic disorders impact how the face forms in some way and thus should be detectable with the assistance of facial recognition technology.[19]

---

12. *Id.* The new computer software was developed by Christoffer Nellåker and Andrew Zisserman of the University of Oxford, along with their colleagues. *Id.* It was designed to assist doctors in making a preliminary diagnosis of rare diseases. *Id.*

13. *Id.*

14. *See* Marie Ellis, *Rare Genetic Disorders Diagnosed by Computer Analysis of Photos*, MED. NEWS TODAY (June 24, 2014), http://www.medicalnewstoday.com/articles/278708.php.

15. Josh Clark, *Does the Shape of My Face Show that I Have a Genetic Disorder?*, HOW STUFF WORKS, http://science.howstuffworks.com/life/genetic/dysmorphology.htm (last visited Feb. 17, 2016).

16. *See* Weller, *supra* note 1.

17. *Id.* According to Nellåker, "it's not sufficiently accurate to provide a rock-solid diagnosis, but it helps narrow down the possibilities." *Id.*

18. *Diagnose Rare Disorders Using Photos*, DECCAN CHRON. (June 25, 2014), http://www.deccanchronicle.com/140625/lifestyle-health-and-wellbeing/article/diagnose-rare-disorders-using-photos. Additionally, "[a] diagnosis of a rare genetic disorder can be a very important step" and "can provide parents with some certainty and help with genetic counseling on risks for other children or how likely a condition is to be passed on," according to lead researcher Nellåker. *Id.*

19. Brian Stallard, *Face Recognition Software Diagnoses Rare Disorders*, NATURE WORLD NEWS (June 24, 2014, 4:05 PM), http://www.natureworldnews.com/articles/7746/20140624/new-face-

B. FRT and Aging

Additionally, scientists are working on a program that analyzes a person's future outlook based on the aging of her face.[20] The technology involves using of a computer to scan pictures of faces for signs of aging based on various factors.[21] Biodemographer Jay Olshansky, professor of computer science Karl Ricanek,[22] and other computer scientists created the program to analyze photographs of faces.[23] The group started a website[24] that invites people to submit a photo and biographical information, which will be analyzed for the return of feedback on their aging-rate calculations and longevity prospects.[25] The technology is more personalized than other current approaches to face-aging analysis, by using different algorithms based on gender and ethnic group.[26]

There are some practical concerns with such uses, such as the reliability of the data.[27] However, Olshansky is optimistic regarding the new technology, stating that an individual's face is a window to her overall health.[28] "The face

---

recognition-software-diagnoses-rare-disorders.htm.

20. Tara Bahrampour, *Can Your Face Reveal How Long You'll Live? New Technology May Provide the Answer*, WASH. POST (July 2, 2014), http://www.washingtonpost.com/national/health-science/can-your-face-reveal-how-long-youll-live-new-technology-may-provide-the-answer/2014/07/02/640bacb4-f748-11e3-a606-946fd632f9f1_story.html. Aging has become a "boom topic" for many entities as people in the United States continually live longer, and research into the number of healthy years involved in the aging process has become a topic for many researching institutes. *Id.* For example, companies such as Google and Human Longevity have launched new programs focusing on aging and age-related diseases, and the National Institutes of Health have also recently started an initiative addressing aging and longevity. *Id.*

21. *See id.* ("Factoring in the subject's race, gender, education level and smoking history—all known to affect longevity prospects—it would analyze each section of cheek, eye, brow, mouth and jowl looking for shading variations that signal lines, dark spots, drooping and other age-related changes that might indicate how the person is doing compared with others of the same age and background.").

22. *See id.* (addressing Professor Ricanek's work on facial recognition technology for the National Security Agency, the CIA, and the FBI).

23. *Id.*

24. FACE MY AGE, http://www.facemyage.com/ (last visited Mar. 1, 2016); *see* Bahrampour, *supra* note 20 ("[The website] is expected to deliver increasingly more accurate assessments and predictions as more people participate. The researchers are hoping for large numbers of people—at least 10,000 or 20,000, but preferably more—to submit photos.").

25. *See* Bahrampour, *supra* note 20.

26. *See id.* (detailing Professor Ricanek's examples that the skin of individuals with lighter complexion tends to age more quickly and women's faces tend to age more quickly than men's).

27. *See id.* (discussing Olshansky's concession that even if face aging is found to correlate with longevity, there will be outliers who do not fit the general pattern).

28. *See id.*

picks up a lot of risk factors for health, such as tobacco smoking (wrinkles around the mouth); excessive alcohol consumption (larger nose); and excessive exposure to the sun (early brown spots and wrinkling) as well as stress," according to Olshansky.[29] The hope is that as individuals receive feedback on their own age analysis, it will contribute to the adoption of individual good, healthy habits, ultimately resulting in longer life spans.[30]

These two examples are just the tip of the iceberg. FRT is advancing at a breakneck pace, and more medical and health applications of FRT are inevitable. In the next Part, I discuss how medical applications of FRT raise different privacy and ethical concerns than FRT for security or commercial purposes.

The Patient Protection and Affordable Care Act (ACA) in part amends the Public Health Service Act[31] in addressing wellness programs "intended to encourage workplace health promotion and prevention as a means to reduce the burden of chronic illness, improve health, and slow the growth of health care costs."[32] Wellness programs are defined by the Public Health Service Act as programs intended to "promote health or prevent disease."[33] Under the ACA, various types of programs available through employer-based group health plans must meet certain requirements, and these programs vary from benefits promoting healthy lifestyles to disease management.[34] Specifically, the ACA addresses the ability of employers to reward employee participation in group health-plan wellness programs, which require employees to meet certain health goals.[35]

Section 2705(j) of the Public Health Service Act, as amended by the ACA, increases the acceptable value of wellness incentives and gives discretion to

29. *Id.*

30. *See id.*

31. Office of the Assistant Sec'y for Planning and Evaluation, *Report to Congress on Workplace Wellness*, U.S. DEP'T HEALTH & HUM. SERVICES [hereinafter Office of the Assistant Sec'y], http://aspe.hhs.gov/hsp/13/WorkplaceWellness/rpt_wellness.cfm (last visited Feb. 24, 2016). The ACA specifically amended the definition of a "wellness program" in section 2705(j)(1)(A) of the Public Health Service Act.

32. *Id.*

33. 42 U.S.C. § 300gg-4(j)(1)(a) (2012); Office of the Assistant Sec'y, *supra* note 31.

34. Office of the Assistant Sec'y, *supra* note 31 ("[T]here is a wide array of workplace wellness programs which include employment-based activities or employer-sponsored benefits aimed to promote health-related behaviors (primary prevention or health promotion) and disease management (secondary prevention).").

35. *Id.*

various government departments to determine if further increases are appropriate.[36] The final rules regarding employment-based, group health-plan wellness programs were published in May 2013.[37] The rule increases the permissible rewards for "health-contingent wellness program[s]" from twenty to thirty percent of the cost of coverage, as well as permitting a maximum reward of fifty percent for programs that target tobacco cessation.[38] This rule also sought to clarify the consumer protections that are required for these wellness programs.[39]

Also applicable in employment-based wellness programming is section 2713 of the Public Health Service Act, which addresses preventive services covered without cost-sharing.[40] This section "requires non-grandfathered group health plans to cover a series of recommended preventive services without imposing cost-sharing, including diet counseling for adults at a higher risk for chronic disease, cholesterol screening for adults of certain ages or at a higher risk, and blood pressure screening," including recommendations for tobacco cessation programming.[41]

C. Implementation of Wellness Programs

Ordinarily, wellness programs include educating about health-related issues, encouraging healthy lifestyle maintenance, and promoting healthier choices.[42] Typical programs include health-risk assessments, behavior modification programs, and lifestyle education programs.[43] Some research indicates that employee participation in wellness programming decreases the

36. 42 U.S.C. § 300gg-4; *see* Office of the Assistant Sec'y, *supra* note 31 ("[This section] raises the allowable value of wellness incentives provided through employment-based group health coverage that require satisfaction of a health-related standard from 20 percent to 30 percent of the cost of coverage in 2014 and provides discretion to the secretaries of DOL, HHS, and the Treasury to increase the reward to up to 50 percent of the cost of coverage if they determine that such an increase is appropriate. It also codifies in statute the HIPAA regulatory standards for health contingent wellness programs.").

37. Office of the Assistant Sec'y, *supra* note 31.

38. *Id.*; *see* 45 C.F.R. § 146.121(f) (2015).

39. Office of the Assistant Sec'y, *supra* note 31.

40. *Id.*; 29 C.F.R. § 2590.715-2713 (2015).

41. *See* 29 C.F.R. § 2590.715-2713; Office of the Assistant Sec'y, *supra* note 31.

42. Laura Anderko et al., *Promoting Prevention Through the Affordable Care Act: Workplace Wellness*, CENTERS DISEASE CONTROL (Dec. 13, 2012), http://www.cdc.gov/pcd/issues/2012/12_0092.htm.

43. Julia James, *Workplace Wellness Programs*, HEALTH POL'Y BRIEFS (May 16, 2013), http://www.healthaffairs.org/healthpolicybriefs/brief.php?brief_id=81.

cost of healthcare.[44] These wellness programs must comply with various state and federal laws, including the ADA, GINA, and HIPAA.[45] However, the ACA regulations regarding wellness programs specifically state that the regulations do not address the application of different laws to wellness programs.[46]

Final ACA regulations separate wellness programming into two categories: (1) "participatory wellness programs" and (2) "health-contingent wellness programs."[47] Participatory wellness programs are "defined under the final regulations as programs that either do not provide a reward or do not include any conditions for obtaining a reward that are based on an individual satisfying a standard that is related to a health factor."[48] Health-contingent wellness programs, in contrast, "require an individual to satisfy a standard related to a health factor to obtain a reward (or require an individual to undertake more than a similarly situated individual based on a health factor in order to obtain the same reward)."[49] This may be performing an activity relating to a health factor or reaching a specific outcome relating to one's health.[50]

Health-contingent programs are divided into two categories: (1) "activity-only wellness programs" and (2) "outcome-based wellness programs."[51] Under an activity-only program, an employee is only required to complete the activity involved, and it does not require the attainment of a specific health outcome.[52]

---

44. *See id.* ("A review of thirty-six peer-reviewed studies of wellness programs in large firms found that average employer medical costs fell $3.27 for every dollar spent on wellness programs, and costs for days that employees were absent fell an average of $2.73. Similarly, a 2005 meta-analysis of fifty-six published studies of health promotion programs at organizations of all sizes resulted in an overall reduction of about 25 percent in sick leave, health plan costs, and workers compensation and disability costs.").

45. *Id.*

46. Incentives for Nondiscriminatory Wellness Programs in Group Health Plans, 78 Fed. Reg. 33,158, 33,158 (June 3, 2013) (to be codified at 45 C.F.R. pt. 146–47).

47. *Id.*

48. *Id.* at 33,160. Examples include:

> (1) A program that reimburses employees for all or part of the cost of membership in a fitness center; (2) a diagnostic testing program that provides a reward for participation and does not base any part of the reward on outcomes; and (3) a program that provides a reward to employees for attending a monthly, no-cost health education seminar.

Id. at 33,160–61.

49. *Id.* at 33,161.

50. *Id.*

51. *Id.*

52. *Id.* ("Examples of activity-only wellness programs include walking, diet, or exercise programs.").

With an outcome-based program, "an individual must attain or maintain a specific health outcome (such as not smoking or attaining certain results on biometric screenings) in order to obtain a reward."[53] The health-contingent programs are acceptable under the ACA if they meet five requirements: (1) eligible individuals have the opportunity to qualify for the reward at least once per year; (2) the total amount of the reward for all activity-only and outcome-based wellness programs combined does not exceed the approved percentages; (3) the program is reasonably designed to promote health or prevent disease; (4) the full reward under both activity-only or outcome-based programs is available to all similarly situated participants; and (5) the plan discloses the availability of a reasonable alternative standard or program for individuals in all plan health-contingent program materials.[54]

D. Concerns About Health-Contingent Wellness Programs

Although supported in the workplace by both employers and employees, there is a conflict regarding the health-based incentive programming that connects rewards to the achievement of a certain health status.[55] One concern voiced by organizations such as the American Heart Association is that this approach may just shift healthcare costs from the healthy to the sick and that the incentives are unfair because not all factors that contribute to a person's health status are under an individual's control.[56] An example of this is genetic predisposition, which can affect numerous different health-status factors, such as excess weight or high blood pressure.[57] Privacy concerns and the discriminatory impact these types of programs could have on the low-income population or racial and ethnic minorities are another concern.[58] Finally, there

53. *Id.*

54. *Id.*

55. James, *supra* note 43.

56. *Id.*

57. *Id.* ("These arguments are some of the reasons the newly proposed federal regulations would require that health-contingent wellness programs must not be overly burdensome on employees, and must also offer a different, reasonable means of qualifying to any person who does not meet the standard based on measurement, testing, or screening.").

58. *Id.* ("These people are more likely to have the health conditions that wellness programs target and also may face more difficult barriers to healthy living. These barriers may include some that are work related, such as having higher levels of job stress; job insecurity; and work scheduling issues. Barriers outside of work may include personal issues, such as financial burdens, and environmental factors, such as unsafe neighborhoods, poor public transportation, and lack of access to healthy food.").

have been concerns raised that the wellness program requirements may actually discourage employee participation because participation may become unaffordable.[59]

Further, there is "ambiguity and inconsistency" between the ACA and the ADA.[60] The question posited is whether "a plan that varies premiums by 30 percent [is] truly voluntary? Might such a plan violate the ADA, even if it was authorized by the ACA?"[61] An example of this concern is found in a current lawsuit filed by the EEOC on behalf of an employee who was allegedly fired for refusal to participate in a health assessment.[62] Normally, employees are given incentives to participate in such programs, but in this case it is alleged that failure to participate in the assessment would result in the employer no longer covering any insurance premiums.[63] The EEOC's suit on behalf of the employee states that requiring participation in the assessment and then firing the employee for refusing to participate violated the ADA.[64] The ADA prohibits discrimination against the disabled, which includes "subjecting workers to 'medical examinations and inquiries.'"[65] However, not all "medical examinations and inquiries" are banned under the ADA, and voluntary health assessments are usually allowed.[66] But in this case, the voluntariness was questioned because there was a lack of meaningful choice for participation in this particular wellness program.[67]

E. New Areas Addressed in the Context of FRT

The Centre for Machine Vision[68] is a company seeking to evolve human–

59. *Id.*

60. Anthony Brino, *Do ACA Wellness Programs Violate Other Federal Laws?*, GOV'T HEALTH IT (Oct. 30, 2014), http://www.govhealthit.com/news/do-aca-wellness-programs-violate-other-federal-laws.

61. *Id.*

62. Nicholas Bagley, *When Are Wellness Programs Illegal?*, INCIDENTAL ECONOMIST (Aug. 22, 2014, 9:25 AM) (citing *EEOC Lawsuit Challenges Orion Energy Wellness Program and Related Firing of Employee*, U.S. EQUAL EMP. OPPORTUNITY COMMISSION (Aug. 20, 2014), http://www.eeoc.gov/eeoc/newsroom/release/8-20-14.cfm), http://theincidentaleconomist.com/wordpress/when-are-wellness-programs-illegal/.

63. *Id.*

64. *Id.*

65. *Id.*

66. *Id.*

67. *Id.*

68. *BRL Centre for Machine Vision (CMV)*, U. W. ENG., http://www1.uwe.ac.uk/et/mvl (last visited Mar. 15, 2016). CMV (formerly Machine Vision Laboratory) is part of the Bristol Robotics Laboratory

computer interaction technology to new contexts.[69] The Centre has developed use of "machine vision" to measure skin cancer growth, detect concealed weapons, and identify changes in human emotions.[70] The Centre has started to work on a new project that uses facial recognition technology to identify changes in mood, which would hypothetically allow measurement of certain facial characteristics that may be able to identify people suffering from depression because they are thought to display different facial characteristics.[71] "This could also have major benefits on caring for the elderly or ill in their homes."[72]

Listed on the website as "coming soon,"[73] WanderID is an application of facial recognition technology by Tactical Information Systems (TIS)[74] that will be an identification system for at-risk individuals.[75] The smart phone app will allow caregivers to upload a picture to TIS, who will put it into a secure database to be accessible by law enforcement and first responders.[76] "When first responders find an unidentified individual, they can take a photo using their smartphone, upload it to WanderID cloud servers, and the TIS database can match the facial characteristics within minutes—with upwards of 99 percent accuracy."[77] Thus, biometrics such as facial recognition may be able "to help rescuers identify lost and confused people who have wandered away from nursing homes or group care facilities" with this new technology.[78]

(BRL), a major research collaboration between the University of the West of England and the University of Bristol. *Id.*

69. *4D Vision - Enabling Computers to Detect Human Emotions*, U. W. ENG., http://www1.uwe.ac.uk/press/uwefeatures/4dvision.aspx (last visited Mar. 15, 2016).

70. *Id.*

71. *Id.*

72. *Id.*

73. *See* WANDER ID, http://wanderid.com/ (last visited Feb. 25, 2016).

74. TACTICAL INFO. SYSTEMS, http://www.tacticalinfosys.com/index.html (last visited Feb. 25, 2016).

75. Kevin Benz, *Biometric Matching in the Cloud: Tactical Information Systems Can Find You*, CULTURE MAP (Jan. 30, 2012, 8:00 AM), http://austin.culturemap.com/news/innovation/01-27-12-13-17-biometric-matching-in-the-cloud-tactical-information-systems-can-find-you/.

76. *Id.*

77. *Id.*

78. Heather Fraser, *Can Wellness Devices Really Improve Health?*, HEALTHCARE GLOBAL (Aug. 31, 2011), http://www.healthcareglobal.com/tech/1195/Can-wellness-devices-really-improve-health.

III. ETHICAL AND POLICY CONCERNS RELATED TO THE MEDICAL AND HEALTH APPLICATIONS OF FACIAL RECOGNITION TECHNOLOGY

Healthcare is one the most highly regulated industries.[79] There are many reasons for this. But one of the reasons is that health information is private, and the government wants to ensure that it is not used in a way that is contrary to public policy.[80] Genetic health information is subject to even more scrutiny than other health information, due to the highly personal nature of such information. When FRT begins delving into the healthcare and medical arena, there is potential for good[81] but also potential for misuse. This Part focuses on the specific privacy concerns in the medical use of FRT: (1) use of this information by employers or others in positions of power and (2) unique privacy concerns with genetic diseases.

A. FRT and Aging: Ethical and Policy Concerns

Although the FRT research introduced above is new, one can easily imagine how this technology could be used for good or nefarious purposes. With regards to the FRT and aging software, on the positive side, individuals who are not aging "well" may give up smoking or start exercising to slow their aging process.[82] However, employers could use these programs in employee wellness programs, and life, disability, and long-term care insurance companies could potentially use this technology in determining premiums. Also, as the opening hypothetical intimates: "If at age 40 if there were something about your face saying you're not likely to make it past 60, an employer could say, 'Oh, I'm not willing to promote you to some position of importance because it's not likely to be a good investment.'"[83] After the advent of the Affordable Care Act, insurance companies can no longer discriminate based on pre-existing conditions, but it is not clear that "aging badly" would qualify as a pre-

79. *An Unhealthy Burden*, THE ECONOMIST (June 28, 2007), http://www.economist.com/node/9407716.

80. *See* Health Insurance Portability and Accountability Act of 1996, 29 U.S.C. § 1181 (2012); *see also Your Rights Under HIPAA*, U.S. DEP'T HEALTH & HUM. SERVICES, http://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html (last visited Mar. 15, 2016).

81. Adam Rubenfire, *Innovations: Facial Recognition Software Measures Pain*, MOD. HEALTHCARE (June 27, 2015), http://www.modernhealthcare.com/article/20150627/MAGAZINE/306279948.

82. Fraser, *supra* note 78.

83. *Id.*

existing condition.[84] Although these are concerns, the use of FRT in genetic screening brings up a myriad of complex issues.

As FRT further develops, it could become commonly used for health and insurance purposes.[85] Although ERISA prevents individual underwriting to determine premiums in employer-based plans, this information could still be used in employer wellness programs and for life insurance, disability insurance, and long-term care insurance policies.[86] Although the accuracy of this technology will not be known for some time, ethical concerns about FRT in the medical and insurance context are being raised now.[87]

B. FRT and Genetic Diagnosis: Ethical and Policy Concerns

The FRT software that can genetically screen faces has the potential for good. With the use of this new program, a disease may be diagnosed earlier and parents may be able to treat diseases and decide whether or not they will have more children based on this information.[88] Additionally, adults who are exhibiting certain symptoms that cannot be explained may be able to receive information from the differential diagnosis that helps tailor their case. However, many carriers of genetic conditions are asymptomatic.[89] In these cases, there may not be a benefit to the knowledge gained by the FRT software.

The right not to know one's genetic disposition is a controversial issue.[90]

---

84. *See The 80/20 Rule and Other Health Care Cost Measures*, UPMC (Oct. 28, 2014), http://www.yourhealthcaresimplified.org/news/80-20-rule-other-health-care-cost-measures/.

85. Liz Klimas, *Why Insurance Companies Are Interested in Facial Recognition Technology*, THE BLAZE (July 3, 2014), http://www.theblaze.com/stories/2014/07/03/why-insurance-companies-are-interested-in-facial-recognition-technology/.

86. *Id.*

87. *Id.*

88. When this software is ready for widespread use, it should be accompanied by genetic counseling. Karen Heller, *Genetic Counseling: DNA Testing for the Patient*, NAT'L CTR. FOR BIOTECHNOLOGY INFO. (Apr. 2005), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1200714/. Although such counseling gives individuals important understanding about medical implications, it does not come without repercussions. *Id.* Genetic testing is foreboding to some, resulting in anxiety and guilt. *Id.* Also, family dynamics can be affected and can result in strained relationships. *Id.* Additionally, there is concern that even with genetic counseling and subsequent testing, there is still misunderstanding and misinterpretation of the results. *Id.*

89. For example, persons who are only carriers of cystic fibrosis do not experience symptoms. *See Carrier Testing for CF*, CYSTIC FIBROSIS FOUND., https://www.cff.org/What-is-CF/Testing/Carrier-Testing-for-CF/ (last visited on Feb. 25, 2016).

90. Graeme Laurie, *Recognizing the Right Not to Know: Conceptual, Professional, and Legal Implications*, 42 J.L. MED. & ETHICS 53, 53 (2014).

The concern is about whether and how genetic information is communicated to individuals and what possible detrimental effects such information can have on individuals.[91] These debates are often centered on the question of whether individuals have a right to know or a right not to know their genetic information.[92] Some people prefer not to know information about their genetic predispositions or diseases and learning about such information could actually cause them harm.[93] For example, it is possible in some situations that an individual could maintain better control over his life by not having the information than by having it.[94] "The more information that might be generated about the individual—due to progress in genetics and proteomics or the expansion of health registers, for instance—the more important it may seem to grant the individual means to avoid it in order to respect autonomy and minimize potential harm."[95]

If the FRT is used on babies and children, there is a real policy issue about these minors having a right not to know.[96] Genetic testing on minors is only

91. Clarissa Allen, Karine Sénécal & Denise Avard, *Defining the Scope of Public Engagement: Examining the "Right Not to Know" in Public Health Genomics*, 42 J.L. MED. & ETHICS 11, 11 (2014).

92. Gert Helgesson, *Autonomy, the Right Not to Know, and the Right to Know Personal Research Results: What Rights Are There, and Who Should Decide About Exceptions?*, 42 J.L. MED. & ETHICS 28, 29 (2014).

93. W. Peter Guarnieri, *Prince Harry and the Honey Trap: An Argument for Criminalizing the Nonconsensual Use of Genetic Information*, 48 AM. CRIM. L. REV. 1789, 1792 (2011). This is particularly the case in situations of incidental findings, when a physician finds something unexpected. Meredith Salisbury, *Should You Have the Right Not to Know Genetic Information?*, FORBES (Nov. 5, 2013), http://www.forbes.com/sites/techonomy/2013/11/05/should-you-have-the-right-not-to-know-genetic-information/. If one applies for a job and then the FRT reveals a genetic pre-condition, this could be seen as an incidental finding. *See id.* There is an issue regarding whether a person affected wants to know the additional information and whether he should have the right to know (or not know) the results. *Id.* Some advocates say that the correct answer is to only disclose the requested results, while others say there is a duty to disclose all results. *Id.* In 2013, this debate rose to a higher level when the American College of Medical Genetics and Genomics (ACMG) announced that this information was to be disclosed to patients who expressly rejected disclosure. *Id.* However, since then, the ACMG has changed its recommendations. *Id.*

94. *See* Helgesson, *supra* note 92, at 33.

95. *See id.* at 30. In addition to the potential harm to individuals, there are also concerns for family members who share the same DNA. Gabrielle Kohlmeier, *The Risky Business of Lifestyle Genetic Testing: Protecting Against Harmful Disclosure of Genetic Information*, 2007 UCLA J.L. & TECH. 5, 24 (2007). Disclosure could result in anxiety, strained familial relationships, and stigmatization. *Id.* There is also a potential "ripple effect" of genetic diseases, and thus, information within family members, including partners and spouses of family members, can result in implications in reproduction. Laurie, *supra* note 90, at 55.

96. *See* Pascal Borry, Mahsa Shabani & Heidi Carmen Howard, *Is There a Right Time to Know? The Right Not to Know and Genetic Testing in Children*, 42 J.L. MED. & ETHICS 19, 20 (2014).

advised when "established, effective, and important medical treatment" exists or when testing "provides scope for treatment which to any essential degree prevents, defers or alleviates the outbreak of disease or the consequences of the outbreak of disease."[97] This principle should apply in the case of FRT as well. If FRT reveals a high likelihood of an incurable disease for which there is no treatment, it is easy to argue that perhaps the child is better off without knowledge of the disease. Once they are adults, they can make their own informed choice regarding such testing.[98]

"Incidental findings—traditionally defined as results that arise that are outside the original purpose for which the test or procedure was conducted—can create a range of practical, legal, and ethical challenges for recipients and practitioners."[99] An incidental discovery can be lifesaving in some contexts, but in others it "can lead to uncertainty and distress without any corresponding improvement in health or wellbeing."[100] Patients may also vary greatly in their beliefs. Additionally, there are no current federal or state statutes that directly address the duty to disclose incidental findings, recognizing that the context in which this has been very briefly addressed is medical malpractice[101] and stating that the legal standard of care may be implicated regarding incidental findings.[102] In the research context, the Commission again noted that no federal law or regulation or any state law specifically addressed disclosure of incidental findings but also recognized that certain federal regulations could be applicable if the context of disclosure was further defined.[103] Finally, in the direct-to-

97. *Id.*

98. *Id.*

99. PRESIDENTIAL COMM'N FOR THE STUDY OF BIOETHICAL ISSUES, ANTICIPATE AND COMMUNICATE: ETHICAL MANAGEMENT OF INCIDENTAL AND SECONDARY FINDINGS IN THE CLINICAL, RESEARCH, AND DIRECT-TO-CONSUMER CONTEXTS 22 (2013) [hereinafter ANTICIPATE AND COMMUNICATE], http://bioethics.gov/sites/default/files/FINALAnticipateCommunicate_PCSBI_0.pdf.

100. *Id.* at 2.

101. *Id.* at 57–58 ("To date, few reported U.S. medical malpractice cases (as opposed to those settled out of court) have addressed clinician liability for failure to identify or disclose incidental findings. A recent study evaluating this limited body of case law concluded that it is possible that clinicians could face liability for failure to identify or appreciate the significance of an incidental finding, or failure to disclose an incidental finding to the patient or other clinicians, if recognition and disclosure would have prevented or altered the course of future disease. In the 2006 case of *Riley v. Stone*, however, a Rhode Island court found that the defendant neurologist did not breach the standard of care when he failed to further assess an incidental finding that he deemed not to pose a danger to the patient." (citations omitted)).

102. *Id.* at 58.

103. *Id.* at 81–82. This report first discusses The Common Rule, formally titled the "Federal Policy for the Protection of Human Subjects," which is a set of regulations governing research with humans

consumer context, the Commission acknowledged that although there are some state laws that regulate or prohibit direct-to-consumer services, there is no such law directly regulating the disclosure of incidental findings.[104] Further, in a federal regulation context, the Food and Drug Administration (FDA) is responsible for ensuring the safety of approved medical devices, but it typically has no authority to regulate their use.[105]

1. Autonomy

Some argue that the choice of not knowing information about oneself is "an expression of the own choices of an individual, which could be framed as a right to informational self-determination."[106] Under the theory of autonomy, the decision to know or not know information lies with the patient, not with the physician.[107] Patient autonomy allows the rejection of "paternalistic interventions bordering on plain oppression for the sake of the overall good."[108] Thus, if the genetic FRT software is used as a routine matter in certain doctors' or employers' offices in the future and a genetic predisposition is revealed by the person's face, does the healthcare provider or employer need to inform the individual? If an adult individual does not want to know, that decision should be respected.[109]

2. Privacy

Related to autonomy, the theory of privacy related to the decision not to

---

that establishes ethical protections. *Id.* at 81. Specifically, in the informed consent process:

> [T]he Common Rule could require disclosure about the possibility of such findings and any policy for their return. The Common Rule could also require disclosure of particular incidental or secondary findings as "significant new findings developed during the course of the research which may relate to the subject's willingness to continue participation."

Id. (citations omitted). Second, the report addresses HIPAA and individuals' rights to receive individual medical information upon request, which could be implicated. *Id.* The report also addresses CLIA, a set of federally mandated standards for lab testing of humans, over which there is currently disagreement about whether incidental findings can be given to participants. *Id.* at 81–82.

104. *Id.* at 98.

105. *Id.* at 98–99.

106. Borry et al., *supra* note 96, at 21.

107. *Id.*

108. Helgesson, *supra* note 92, at 30.

109. *See id.*

know rests on the concept of "control."[110] Privacy advocates worry about "unsolicited revelations of personal information" and recognize that such actions may result in an invasion of privacy.[111] The theory of privacy addresses a broader spectrum of issues than autonomy, including the security of health information and addressing situations such as the trust relationship established between patients and doctors or participants and researchers.[112]

3. International Guidance

The "right not to know"[113] has been recognized by UNESCO in its 1997 Universal Declaration on the Human Genome and Human Rights, which states in Article 5(c): "The right of each individual to decide whether or not to be informed of the results of genetic examination and the resulting consequences should be respected."[114] The 1997 Council of Europe Oviedo Convention on Human Rights and Biomedicine provided that "[e]veryone is entitled to know any information collected about his or her health. However, the wishes of individuals not to be so informed shall be observed."[115]

110. Borry et al., *supra* note 96, at 21–22.

111. *Id.* (quoting ALLEN E. BUCHANAN & DAN W. BROCK, DECIDING FOR OTHERS: THE ETHICS OF SURROGATE DECISION MAKING (1989)).

112. *See* Laurie, *supra* note 90, at 61 ("[I]f participants cannot always negotiate and defend their own interests, then they must trust that others do this on their behalf. Recognizing the possibility of the interest in not knowing adds an important and powerful dimension to the trust relationship.").

113. Borry et al., *supra* note 96, at 20.

114. UNESCO, RECORDS OF THE GENERAL CONFERENCE: TWENTY-NINTH SESSION: RESOLUTIONS 41 (1997), http://unesdoc.unesco.org/images/0011/001102/110220e.pdf; *see* Borry et al., *supra* note 96, at 20; Laurie, *supra* note 90, at 53.

115. COUNCIL OF EUROPE, CONVENTION FOR THE PROTECTION OF HUMAN RIGHTS AND DIGNITY OF THE HUMAN BEING WITH REGARD TO THE APPLICATION OF BIOLOGY AND MEDICINE: CONVENTION ON HUMAN RIGHTS AND BIOMEDICINE 3 (1997); *see* Borry et al., *supra* note 96, at 20; Laurie, *supra* note 90, at 53. An additional example is the Dutch Civil Code, which states: "[I]f the patient indicates that he does not want to receive information, then this is not provided, unless the potential resulting prejudice to himself or others outweighs the patient's interest in not knowing." Charles E. Maclean, *Creating a Wanted Poster from a Drop of Blood: Using DNA Phenotyping to Generate an Artist's Rendering of an Offender Based Only on DNA Shed at the Crime Scene*, 36 HAMLINE L. REV. 357, 382 (2013) (citations omitted). Further, the right not to know has been recognized in the context of minors by the British Society for Human Genetics guidelines by advising that "testing should normally be delayed until the young person can decide for him/herself when, or whether, to be tested." *See* Borry et al., *supra* note 96, at 21.

IV. REGULATION OF FACIAL RECOGNITION TECHNOLOGY: FTC AND INDUSTRY GUIDANCE

The Federal Trade Commission (FTC) released a comprehensive report in 2012 entitled *Facing Facts, Best Practices for Common Uses of Facial Recognition Technologies*, which considered the beneficial uses to consumers of FRT and the privacy issues that need to be researched with the expansion of the commercial use of such technology.[116] The FTC recognized that the FRT industry will continue to expand, discussed how the technologies are being used, examined foreseeable future uses, and advised about the possible risks and benefits of the technology.[117] What is interesting is that none of the described commercial uses involved medical or health applications. However, the Report is still instructive for FRT for medical and health purposes.

The Report identified best practices for the commercial use of FRT: privacy by design, simplified consumer choice, and transparency.[118] Numerous professional groups participated in the Face Facts workshop, during which discussion arose on the major topics involved in facial recognition technology: "(1) recent advances in [the] technolog[y], (2) current commercial uses . . . , (3) possible future uses . . . , and (4) privacy concerns."[119]

A. Recent Advances in FRT

In the Report, the FTC acknowledged that the commercial use of FRT is becoming more prevalent due to lower costs and higher accuracy.[120]

116. FED. TRADE COMM'N, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES 1–2 (2012) [hereinafter FACING FACTS REPORT], http://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf. The Report stemmed from the FTC's Face Facts workshop in December 2011, which initially discussed the uses of FRT and the impact on consumers. *Id.* at 1. The workshop was followed by a period of public comment, which was used to help develop the recommended best practices for the commercial use of the facial recognition technology. *Id.*

117. *Id.*

118. *See id.* at 1–2 (citing FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE, RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS (2012), http://www.ftc.gov/os/2012/03/120326privacyreport.pdf).

119. *See id.* at 3. "Researchers, academics, industry representatives, and consumer and privacy professionals" were all a part of the workshop discussions. *Id.* The developments discussed were "technologies that merely detect basic human facial geometry; technologies that analyze facial geometry to predict demographic characteristics, expression, or emotions; and technologies that measure unique facial biometrics." *Id.*

120. *See id.* at 3–4 ("For example, from 1993 to 2010, tests conducted by the National Institute of

Previously, programs utilizing FRT were unlikely to match two images of the same person "if the photos were taken from different angles."[121] However, the Report describes how many companies use 3D images to solve this issue.[122] Several of the technological advancements are attributed to the increase in availability of online photographs.[123] The Report cites Facebook as an example, noting that consumers uploaded 2.5 billion photos in a single month in 2010.[124]

B. Current Commercial Uses of FRT

The Report does not anticipate the commercial medical or health uses of FRT. However, the Report is still instructive. It describes various current uses, from general facial detection technologies[125] to specific identification of an individual person.[126] The Report focuses on the current commercial uses of facial detection, such as search engine results,[127] virtual eyeglass fitting systems and makeover tools,[128] and real-time targeted advertising.[129] Real-time targeted

---

Standards and Technology (NIST) showed that the false reject rate—the rate at which facial recognition systems incorrectly rejected a match between two faces that are, in fact, the same—was reduced by half every two years.").

121. *Id.* at 4.

122. *See id.*

123. *See id.* (noting that ten years ago, most online images were of celebrities, while increased social media has led to a huge influx of images of private citizens online).

124. *See id.* ("This multitude of identified images online can eliminate the need to purchase proprietary sets of identified images, thereby lowering costs and making facial recognition technologies commercially viable for a broader spectrum of commercial entities."). Participants in the workshop also mentioned several other developments that have also attributed to the increase accuracy of facial recognition technology, including better digital cameras with higher quality images. *Id.* at 3.

125. *See id.* at 4. This is the ability to detect a face in an image. *Id.* Workshop participants also looked at possible future uses of the technology, most of the conversation focusing on the possibility of using facial recognition to identify anonymous people in public places. *Id.* at 6–7. Although it seems currently impossible for commercial use on a large scale, the FTC referenced studies that suggest it may be possible in the future. *Id.*

126. *See id.* at 4. Specific identification is when an image of a person "is matched with another image of the same individual." *Id.* Thus, "if the face in either of the two images is identified . . . then, in addition to demonstrating a match between two faces, the technology can be used to identify previously anonymous faces." *Id.* The middle ground between these two types of technology also encompasses determining facial characteristics that are attributed to "age, gender, and recognizing emotions." *Id.*

127. *See id.* at 5 ("[R]efining search engine results to include only those results that contain a face, locating faces in images in order to blur or de-identify them, or ensuring that the frame for a video chat feed actually includes a face.").

128. *See id.* A consumer uploads a "selfie" to the website, where basic facial features are used to superimpose the product on the consumer's face. *See id.*

advertising benefits advertisers because it expands their targeted audience and could lead to more sales.[130] The FTC discussed SceneTap as an example, which uses FRT to capture age range and gender of clientele at bars and nightclubs to determine demographics and could provide helpful information to venue operators and third-party vendors to target their promotions.[131]

The Report also discussed how FRT is being used for authentication purposes[132] and on social network sites.[133] The most widespread use of the comparison and identification technology in FRT is to implement semi-automatic "tagging" on social network sites in photo management and applications.[134] The existing system is limited to suggestions of "'tags' of people that the user already knows" or with whom they have a mutual "friend."[135]

C. Privacy Concerns Raised by the FTC Report

Although many of the examples cited by the FTC demonstrated consumer benefits and even the ability of the commercial entity to protect privacy, the Report documented many privacy concerns.[136] The concerns raised at the workshop included that databases storing the sensitive information may be at risk for hacking, consumers may view targeted facial recognition advertising as an invasion of privacy, and the technology may eliminate the ability for individual anonymity in public places.[137] The third concern delivered the most concern to the participants of the workshop, stemming from "serious privacy

129. *See id.* ("For instance, technologies that identify moods or emotions from facial expressions can be used to determine a player's engagement with a video game or a viewer's excitement during a movie. Further, technologies that can determine the gender and age range of the person standing in front of a camera can be placed into digital signs or kiosks, allowing advertisers to deliver an advertisement in real-time based on the demographic of the viewer.").

130. *Id.*

131. *See id.* at 5–6 ("SceneTap also makes the aggregate information it collects available through a mobile app that consumers can use to make decisions about which venues to patronize."). Although these programs go beyond simply detecting a face in an image, they do not use the "biometric data for comparison purposes." *Id.*

132. *See id.* at 6 ("For example, they can be used for authentication purposes by enabling a mobile phone user to use her face, rather than a password, to unlock her phone.").

133. *Id.*

134. *Id.*

135. *Id.*

136. *Id.* at 7–8.

137. *Id.*

and physical safety concerns."[138]

The FTC requested public comments regarding issues raised on privacy concerns and best practices for the commercial implementation of facial recognition technology.[139] The feedback provided encompassed several underlying themes, including that: (1) "companies should implement privacy protections for all facial recognition technologies"; (2) transparency is necessary, which includes the need for consumer education, especially among teens; and (3) the role of self-regulation and the implementation of industry "best practice" standards.[140] The FTC, in agreeing with the commentary, noted that most of the principles suggested were the same as those suggested in the March 2012 FTC Privacy Report.[141]

Thus, the FTC developed case studies demonstrating how commercial entities could implement the suggested principles when using facial recognition technology.[142] The studies were not intended to provide an exhaustive list of

138. *Id.* at 8. The overarching concern results in the consensus that before implementation of any of the abovementioned technologies, there needs to be implementation of appropriate privacy protections. *Id.* at 7–8.

139. *Id.* at 8; *see FTC Seeks Public Comments on Facial Recognition Technology*, FED. TRADE COMMISSION (Dec. 23, 2011), https://www.ftc.gov/news-events/press-releases/2011/12/ftc-seeks-public-comments-facial-recognition-technology.

140. FACING FACTS REPORT, *supra* note 116, at 9–10.

141. *See id.* at 10 ("[P]rivacy by design, simplified choice, and improved transparency.").

142. *See id.* at 10–20. There were three hypotheticals described by the FTC. In the first scenario, an eyeglass company implements a website which allows consumers to upload their pictures and superimpose different styles of glasses on their face, storing the images for future use by the consumer. *Id.* at 11. According to the FTC, the voluntary photo upload is not the concern, it is the company's storage of the image that raises the issue. *Id.* The best practices suggested by the FTC in this scenario first include implementation of "privacy by design" by protecting the uploaded images. *Id.* at 11–12. Second, the recommendation for implementation of transparency, the company should communicate its use of the data and provide consumer choices in the context of the transaction. *Id.* at 12. An example given by the FTC was to state, at the time of photo upload, information regarding the reasons for storing instead of deleting the photos, etc., further stating, "In all cases, the company should also inform consumers of: (1) the length of time the images are stored, (2) who will have access to the stored images, and (3) consumers' rights regarding deletion of the stored images." *Id.* Third, the FTC recommended that if use of the data changes, the company needs to obtain "affirmative express consent of the consumer." *Id.* As an example, if the eyeglass company decided to use the image for advertising rather than just storing the image for the consumer, it would require affirmative consent. *Id.*

In the second hypothetical, the FTC examines a sports drink company using digital signs in a grocery store to display targeted advertisement to the consumer in front of the sign through assessing age range and gender. *Id.* at 13. In this case, "[t]he consumer's image is processed instantaneously" and is not kept for future use. *Id.* According to the FTC, "privacy by design" should be used to prevent instantaneous system hacking by using data security protections. *Id.* Regarding company transparency, the suggestion is that clear notice that the digital sign contains a camera using facial recognition technology is needed. *Id.* at 15. Consumer choice is also notably important in this hypothetical, clear notice

implementation techniques, but rather to provide an example of suggested best practices.[143] Each of these best practices focused on privacy by design through technological fixes, such as protecting uploading facial images, preventing hacking, protecting user data, and appropriately establishing retention and disposal practices.[144] They also focused on implementation of transparency, consumer choice, and consent.[145] Each of these principles—privacy by design, simplified choice, and improved transparency—can be applied to the FRT for medical and health purposes. FRT for medical and health purposes must ensure the technology is secure, that it is used with patient consent, and those patients know every way that the results will be used. Although this would be better than nothing, the FTC guidance is just that—guidance.

It is interesting that FTC Commissioner Rosch dissented with the issuance of the report.[146] Overall, he felt that the report by the FTC was premature because he did not believe that "such far-reaching conclusions . . . can be justified at this time."[147] Three years later, it seems that the FTC Report was prescient and actually under anticipated some of the uses of FRT. If anything, the new applications of FRT point to the need for even more stringent

---

is applicable so a consumer can choose to avoid the sign. *Id.* Again, if the company decides to use the information in a way other than originally intended, such as collecting the data, the company needs to first obtain affirmative, express consent of the consumer. *Id.* at 16.

The last hypothetical examines a social network that implements facial recognition, specifically regarding user photo uploads, and the network scanning the photos against "tagged" photos of the user's "friends." *Id.* at 17. This system would allow for the site to identify the user's "friends" in new photos for the user to "tag." *Id.* "Privacy by design" is discussed in this scenario as highly important, including the various ways to protect user data, and appropriately establishing retention and disposal practices. *Id.* at 17–18. Transparency and consumer choice are also suggested, by informing the consumer about the network's data practices, and letting the consumer choose whether to participate in the use of facial recognition technology, further stating that consumers need to have the option to turn of the feature anytime, thereby deleting the previously collected biometric data. *Id.* at 18–19. The final suggestion for the social networks is that that it should not collect and store data of non-users because non-users have an absence of choice regarding such practices. *Id.* at 19. Thus, this leads to the conclusion that these networks need to obtain express, affirmative consent from all of those who participate in the program, as only consumers who have affirmatively chosen to participate should be identified. *Id.* at 20.

143. *See id.* at 10–20.

144. *See generally id.* (providing examples of best practices as applied to three case studies).

145. *See id.*

146. *See id.* at A1–A2 (Rosch, Comm'r, dissenting). Rosch disagreed that "best practices" should be adopted by the FTC solely because the technology has a possibility for misuse, stating that it was "at least premature . . . to suggest to businesses that they should adopt as 'best practices' safeguards that may be costly and inefficient against misconduct that may never occur." *Id.* at A2. Rosch opposed the "consumer choice" model implemented in the report, stating it is nearly impossible to establish an exact "consumer[] expectations" test. *Id.*

147. *Id.*

standards. Companies are not required to abide by the recommendations—compliance with the best practices is purely voluntary.[148] The FTC outlines best practices as a guide to company policy regarding facial recognition technology.[149] By utilizing the suggestions, companies can promote consumer trust and ensure industry growth, thus incentivizing additional companies to implement the suggested best practices.[150]

D. Industry Efforts at Self-Regulation

In addition to the FTC's proposed best practices, there have been some limited industry efforts at self-regulation. Because FRT-based interactive marketing will likely be used by the digital sign industry,[151] the Digital Signage Federation (DSF) has set forth recommended industry standards based on the privacy implications involved.[152] Although DSF deals with different aspects of FRT than those related to medical and health practices, some of its analysis is translatable.[153] After examining current privacy protection implementation and industry practices, the DSF noted that these generally extended to "personally identifiable information"[154] traditionally assumed to be the only information that could be directly linked to a person's identity.[155] However, the DSF noted

148. *Id.* at iii ("The recommended best practices contained in this report are intended to provide guidance to commercial entities that are using or plan to use facial recognition technologies in their products and services.").

149. *Id.* (noting that the recommended best practices "are not intended to serve as a template for law enforcement actions or regulations").

150. *Id.* at 21.

151. *See* DIG. SIGNAGE FED'N, DIGITAL SIGNAGE PRIVACY STANDARDS 1 (2011), http://www.digitalsignagefederation.org/Resources/Documents/Articles%20and%20Whitepapers/DSF%20Digital%20Signage%20Privacy%20Standards%2002-2011%20%283%29.pdf ("Through technologies and platforms like mobile marketing, social networking, facial recognition and radio frequency identification, digital signage companies can personalize message content, build customer relationships, streamline network management and provide accountability to advertising clients.").

152. *Id.*

153. *Accord id.* (suggesting the recommendations are focused on "preserv[ing] public trust . . . . [and] prevent[ing] privacy risks"). The goals and motivations at the heart of the Digital Signage Federation's suggestions mirror those discussed in this article with regard to medical uses of FRT. *Id.*; *see also supra* Part III.A.

154. *See* DIG. SIGNAGE FED'N, *supra* note 151, at 1–2. Also known as "directly identifiable data," typically including name, address, phone number, date of birth, social security number, driver's license number, license plate number, email address, account numbers, or "biometric data, such as unique data points captured via facial recognition systems [and] [i]mages or voice recordings of individuals." *Id.* at 2.

155. *Id.* at 1–2.

that the distinction between information that is personally identifiable and information that is not is becoming less meaningful as technology progresses.[156] The DSF recommended that privacy protections also extend to "pseudonymous data,"[157] or data that does not directly identify an individual but can be traced to a person's identity relatively easily.[158] This concept is important and should extend to FRT for medical or health purposes as well.

The DSF proposed eight separate policy considerations to assist in promoting privacy protection. These include transparency,[159] individual participation,[160] purpose specification,[161] data minimization,[162] use limitation,[163] data quality and integrity[164] security,[165] and accountability.[166] The guidelines set forth by the DSF are based on internationally recognized principles outlined in the Fair Information Practices, which the DSF explains are incorporated both in privacy laws in the United States and the European Union's Data Protection Directive.[167] In addition to recommending general guidelines, the DSF further

156. *Id.*

157. *See id.* at 2. This data includes RFID codes; device identification numbers, such as IP addresses; internet usernames; social networking data; and data a user enters knowingly. *Id.* The report suggests the need for protection over information so easily used to identify an individual. *Id.*

158. *Id.*

159. *Id.* at 4–6. This refers to the two principal ways of implementation: through development of "concise and specific" privacy policies to be published on companies' websites and specific notice at the location of the digital sign. *Id.*

160. *See id.* at 6–8. Individual participation refers to the individual's right to consent to the collection and use of their data, and the right to access the collected data. *Id* at 6. The DSF examines the three general ways information is collected—audience counting, audience targeting, and audience identification and profiling—and how the system operates and how consent should be obtained in each scenario. *Id.* at 6–8.

161. *See id.* at 8. This refers to the recommendation that companies disclose the intended use of the data collected through privacy policies. *Id.*

162. *Id.* Data minimization refers to the collection and retention of data. *Id.* The DSF proposes that companies collect "only the minimum amount they need to achieve specified ends," and that the data collected should be kept no longer than necessary. *Id.*

163. *Id.* The DSF proposes that companies not use or share the collected data in a way that is not disclosed in the company's privacy policies. *Id.*

164. *Id.* at 9. The DSF suggests that data quality and integrity can be ensured through consumer access and best practices. *Id.* The data should be "accurate, relevant, timely, and complete." *Id.*

165. The DSF identifies employee access, systems security, and database retention principles as key aspects of a security policy. *Id.* ("The best data security is for a company not to possess consumer data in the first place.").

166. Accountability refers to the fact that companies should implement internal systems to regulate compliance with privacy policies and applicable laws, as well as provide training for employees. *Id.*

167. *Id.* at 4 (providing as an example the "modern formulation of these principles" adopted by the U.S. Department of Homeland Security, including: transparency, individual participation, purpose speci-

proposed that digital signage companies reach out to existing privacy frameworks related to the utilized technologies for use in the development of policies and best practices.[168]

E. CDT

The Center for Democracy and Technology (CDT) has considered the privacy issues involved in FRT.[169] In its 2012 report, the CDT described the privacy concerns in the context of three main levels.[170] Level one is individual counting, where consumer facial information is used as a general recognition mechanism and gathered on an aggregate basis but not stored.[171] The CDT labels this level as the least likely form of FRT to intrude on individual privacy.[172] Level two is individual targeting, in which facial information is used in making targeted advertisements.[173] In this system the information is not retained, but is used, for example, to "record passerby demographics and contextualize ads accordingly."[174] Level three is called individual identification, where the individual's data is collected and facial information is linked to an individual's identity, property, or location.[175]

The CDT argues that current state and federal regulations are not adequate to protect consumers in the FRT arena; most state and federal laws do not address consumer privacy protection of biometric information collected for commercial purposes.[176] Federal law does not explicitly address the use of FRT

---

fication, data minimization, use limitation, data quality and integrity, security, and accountability).

168. *See id.* ("[D]igital signage companies that utilize mobile marketing should use the Mobile Marketing Association (MMA)'s Global Code of Conduct . . . . [C]ompanies that use RFID should integrate the standards of relevant trade associations or privacy groups . . . . [C]ompanies that target advertisements to consumers based on their activities may want to consider the online behavioral advertising guidelines issued by the Network Advertising Initiative and by the Interactive Advertising Bureau . . . [and] companies should be aware of other digital signage privacy guidelines, including the very well done Code of Conduct issued by Point of Purchase Association International.").

169. CTR. FOR DEMOCRACY & TECH., SEEING IS ID'ING: FACIAL RECOGNITION & PRIVACY 1 (2012), https://www.cdt.org/files/pdfs/Facial_Recognition_and_Privacy-Center_for_Democracy_and_Technology-January_2012.pdf.

170. *Id.* at 6.

171. *Id.*

172. *Id.*

173. *Id.*

174. *Id.*

175. *Id.*

176. *Id.* at 9 ("Federal laws—and nearly all state laws—do not provide American consumers with basic privacy protections when it comes to biometric information collected for commercial purposes

in the private sector, although it does provide a legal remedy for the unauthorized use of such information in the context of identity theft or fraud.[177] The CDT suggests that legislative remedies could be introduced that would help in this arena. The CDT believes it would be better if Congress "pass[ed] a strong baseline consumer privacy law,"[178] rather than targeting FRT alone.[179] It suggests that privacy law in the United States is fragmented and "[e]stablishing privacy laws for facial recognition in isolation will perpetuate this fragmentation," leading to ineffective protection for consumers.[180]

F. National Telecommunications & Information Administration 2014 Meetings on FRT

FRT is a topic ripe for discussion because it is rapidly expanding in its sophistication and use. The National Telecommunications & Information Administration (NTIA) of the United States Department of Commerce is another governmental body that is attempting to address FRT.[181] The NTIA held a series of meetings in 2014 regarding the commercial use of FRT.[182] NTIA intended for the meetings and feedback to lead to the development of an

online or offline.").

177. *Id.* (noting further "both the Privacy Act and Office of Management and Budget memoranda cover biometric information held by government agencies.").

178. *Id.* at 13.

179. *Id.* A baseline law could help by "providing consumers with a measure of control over whether they participate in commercial facial recognition systems and requiring companies to be transparent about their use of facial recognition." *Id.* It "should also establish a safe harbor program in which companies that adhere to enforceable industry self-regulatory privacy codes enjoy specified incentives, such as exemption from some forms of liability." *Id.*

180. *Id.* at 13–14.

181. *See* Nat'l Telecomm. & Info. Admin., *Privacy Multistakeholder Process: Facial Recognition Technology*, U.S. DEP'T COM. (June 11, 2015) [hereinafter *Privacy Multistakeholder Process: Facial Recognition Technology*], http://www.ntia.doc.gov/other-publication/2014/privacy-multistakeholder-process-facial-recognition-technology.

182. *Id.*; *see also* Lawrence E. Strickling, *NTIA to Convene First Facial Recognition Technology Mutlistakeholder Meeting*, U.S. DEP'T COM. (Feb. 5, 2014), https://www.ntia.doc.gov/blog/2014/ntia-convene-first-facial-recognition-technology-multistakeholder-meeting. The goal of the meetings was set forth as involving a stakeholder discussion on best practices to "ensure that consumers' rights to control, transparency, security, access and accuracy, focused collection, and accountability are respected within the context of current and emerging commercial uses of facial recognition technology." Nat'l Telecomm. & Info. Admin., *Privacy Multistakeholder Meetings Regarding Facial Recognition Technology: February—June 2014*, U.S. DEP'T COM. (Dec. 3, 2013) [hereinafter *Privacy Multistakeholder Meetings*], http://www.ntia.doc.gov/other-publication/2013/privacy-multistakeholder-meetings-regarding-facial-recognition-technology-feb.

enforceable code of conduct specifying how the Consumer Privacy Bill of Rights applies to the use of FRT.[183] The NTIA acknowledged that FRT has many potential benefits for consumers but also noted that there are serious privacy challenges involved.[184] The NTIA also used the FTC Report and other academic publications in the stakeholder discussion process.[185] Unfortunately,

183. *Privacy Multistakeholder Meetings*, *supra* note 182. The February 25, 2014, meeting discussed proposed cases to be used as examples of how the code of conduct could address the issues involved, including use of facial recognition technology used through surveillance cameras, mobile applications, and kiosks. NAT'L TELECOMM. & INFO. ADMIN., NTIA PRIVACY MULTISTAKEHOLDER PROCESS, COMMERCIAL FACIAL RECOGNITION TECHNOLOGY, PROPOSED USE CASES THAT MIGHT BE ADDRESSED BY A CODE OF CONDUCT 1 (Feb. 21, 2014), http://www.ntia.doc.gov/files/ntia/publications/stakeholder_use_cases_2_21_14.pdf. The subsequent meeting on March 25, 2014, provided a list of documentation to be used as a background resources for the meetings, including the FTC documentation on best practices. NAT'L TELECOMM. & INFO. ADMIN., NTIA PRIVACY MULTISTAKEHOLDER PROCESS, COMMERCIAL FACIAL RECOGNITION TECHNOLOGY, PRELIMINARY BACKGROUND RESOURCES 1 (2014), http://www.ntia.doc.gov/files/ntia/publications/background_resources_facial_recognition_3_24_14.pdf; *see* FACING FACTS REPORT, *supra* note 116, at 4–6. The March 25th meeting also updated the proposed use cases list to twenty-nine scenarios where a code of conduct could be implemented to address concerns arising from the use of facial recognition technology. *See also* NAT'L TELECOMM. & INFO. ADMIN., NTIA PRIVACY MULTISTAKEHOLDER PROCESS, COMMERCIAL FACIAL RECOGNITION TECHNOLOGY, PROPOSED USE CASES THAT MIGHT BE ADDRESSED BY A CODE OF CONDUCT 1 (Mar. 24, 2014), http://www.ntia.doc.gov/files/ntia/publications/stakeholder_use_cases_3_24_14.pdf. Further, this meeting included information provided by IBG, a company involved in independent biometric testing. INT'L BIOMETRIC GRP., FACE PROCESSING IN SOCIAL NETWORKING SERVICES (2014), http://www.ntia.doc.gov/files/ntia/publications/ntia325meetingfinal.pdf. The report was titled *Face Processing in Social Networking Services* and addressed the background facts pertinent to face processing technologies. *Id.* at 3–4. A subsequent conference call on March 26, 2014, provided information on facial recognition in online and mobile services in the European Union. JACOB KOHNSTAMM, EUROPEAN COMM'N, OPINION 02/2012 ON FACIAL RECOGNITION IN ONLINE AND MOBILE SERVICES (2012), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp192_en.pdf. The documentation provided addresses varying uses of facial recognition technology, providing examples specifically in the online and mobile services realms. *Id.* at 1–2. The report provides recommendations for the encountered risks, including: companies providing detailed information, obtaining informed consent, using the data for specified purposes, allowing for consumer access, and adequate security systems. *Id.* at 7–9. These proposals are contextualized by a discussion of the European Union's legal framework, called the Data Protection Directive, which addresses digital images as personal data and the processes involved, as well as providing recommendations for the encountered risks. *Id.* at 3–7.

184. *Privacy Multistakeholder Meetings, supra* note 182. The specific challenges involved include: "(1) securing sensitive biometric data; (2) providing transparency when facial recognition is implemented in retail stores or other public places; and (3) developing meaningful controls for consumers when the source material for facial recognition technology—digital images—is often widely available." *Id.*

185. *See id.* ("These [FTC reports and academic publications] indicate that the facial recognition topic is a strong opportunity for stakeholders to reach consensus on a code of conduct in a reasonable timeframe."). The initial stakeholder meetings were set to start a "factual, stakeholder-driven dialogue" regarding facial recognition technology, how it is currently implemented, how it may be used in the future, and the privacy concerns involved. *Id.* Further meetings were scheduled with the intent to formu-

the meetings to date have not addressed FRT use for medical or health purposes; they have focused instead on concerns about the software security and not about how the information garnered by the FRT is used.[186]

All of the meetings have resulted in interesting conclusions, but the conclusions made at the March 2014 meeting were instructive on privacy issues.[187] The NTIA considered the issue of whether a biometric template stored without other identifying information could still be considered a unique identifier.[188] The participants at that meeting concluded "a face recognition template is [personal identifying information], like any other biometric information."[189] This language is of particular interest because it lends credence to the arguments I make in the HIPAA section below that FRT implicates individually identifiable data.

The NTIA also considered whether breaking into the template, image reconstruction, and template linking would "require a sophisticated attacker with a Ph.D.?"[190] Unfortunately, the answer was that an unsophisticated hacker could do this because the algorithms have already been developed, and all that is needed is the software.[191] This is particularly worrisome in the case of FRT for health or medical use because health information should be afforded the utmost privacy.

At the May 2014 meeting, the stakeholders were more specific and submitted a proposal for principles that may be incorporated into the code of conduct.[192] The ACLU submitted its report, entitled *An Ethical Framework for*

---

lize the code of conduct setting forth privacy practices for the industry. *Id.*

186. *See Privacy Multistakeholder Process: Facial Recognition Technology (2015)*, NAT'L TELECOMM. & INFO. ADMIN. (June 11, 2015), https://www.ntia.doc.gov/other-publication/2015/privacy-multistakeholder-process-facial-recognition-technology (providing agendas, recommendations, and related documents for the meetings held in 2014).

187. MICHELLE CHIBBA & ALEX STOIANOV, INFO. & PRIVACY COMM'N OFFICE OF ONT., CAN., ON UNIQUENESS OF FACIAL RECOGNITION TEMPLATES (2014), http://www.ntia.doc.gov/files/ntia/publications/uniqueness_of_face_recognition_templates_-_ipc_march-2014.pdf.

188. *Id.* at 1–2.

189. *Id.* at 2. The NTIA also considered the question of whether a facial image can "be reconstructed from the template especially if the template generating algorithm is not known . . . ." *Id.* According to the experts at the meeting, approximately 93% of the time this can be done successfully in the system. *Id.* at 3. The meeting also concluded that two facial templates created for the same person but by different algorithms can be linked. *Id.* at 4.

190. CHIBBA & STOIANOV, *supra* note 187, at 4.

191. *Id.*

192. NAT'L TELECOMM. & INFO. ADMIN., NTIA PRIVACY MULTISTAKEHOLDER PROCESS, COMMERCIAL FACIAL RECOGNITION TECHNOLOGY, PROPOSED PRINCIPLES THAT MIGHT BE INCORPORATED INTO A CODE OF CONDUCT (May 16, 2014), http://www.ntia.doc.gov/files/ntia/public-

Facial Recognition.[193] This provided factual findings that pointed to the privacy concerns involved in facial recognition programs, such as the potential for future use of the technology, individual identification, and the possibility of exploitation of teenagers.[194] The ACLU's recommendations included the need to protect "biometric information from exploitation and misuse" and advocated for government intervention and statutory legal protection.[195]

The next Part analyzes health-related regulations to determine whether these regulations protect individuals from privacy breaches that may occur in the use of FRT for medical and health purposes.

V. ANALYSIS OF FRT FOR MEDICAL PURPOSES UNDER HIPAA, GINA, AND THE ADA

A. GINA and FRT For Medical Purposes

GINA was enacted in 2008 with the intent to protect individuals from genetic discrimination, which is defined as the misuse of genetic information.[196]

---

ations/stakeholder_principles_5_16_2014.pdf (including individual control, transparency, respect for context, security, access and accuracy, focused collection, and accountability).

193. ACLU, AN ETHICAL FRAMEWORK FOR FACIAL RECOGNITION 1 (2014), https://www.ntia.doc.gov/files/ntia/publications/aclu_an_ethical_framework_for_face_recognition.pdf.

194. *Id.* at 1–2.

195. *Id.* at 2. Additionally, the Interactive Advertising Bureau has made similar observations regarding the need to carefully protect biometric information and develop a code of conduct that "protects businesses and consumers while allowing for continued innovation." INTERACTIVE ADVERT. BUREAU, IAB PRINCIPLES FOR THE NTIA MULTISTAKEHOLDER PROCESS ON FACIAL RECOGNITION TECHNOLOGY (2014), https://www.ntia.doc.gov/files/ntia/publications/iab_facial_recognition_governing_principles_5.15.pdf. (advocating for a harm-based approach, technology neutrality, security, and a public information exception). The NTIA's June 2014 meeting included recommendations made by the International Biometrics Industry Association (IBIA). INT'L BIOMETRICS INDUS. ASS'N, IBIA PRIVACY BEST PRACTICE RECOMMENDATIONS FOR COMMERCIAL BIOMETRIC USE (2014), https://www.ntia.doc.gov/files/ntia/publications/ibia_statement_to_ntia_-_best_practice_recommendations_6-17-2014.pdf. Transparency and data protection are the IBIA's "fundamental privacy tenets." *Id.* at 1. The IBIA acknowledged two hurdles to crafting best practices recommendations: first, the biometric industry lacks legal authority to impose rules on users of the technology; second, "the variety and numerous existing uses, as well as potential uses [of FRT]" makes creating specific and narrowly tailored recommendations at best impractical. *Id.* The IBIA did advocate for general guidelines that could provide a framework to ease implementation of greater privacy controls in specific contexts, however. *Id.* at 2.

196. Genetic Information Nondiscrimination Act of 2008, Pub. L. No. 110-223, 122 Stat. 881 (codified as amended in scattered sections of 29 U.S.C. and 42 U.S.C.). *See generally* GENETIC INFO. NONDISCRIMINATION ACT, http://www.ginahelp.org/ (last visited Mar. 12, 2016) (providing additional information about the individual protections and importance of the GINA).

GINA involves protection of "family health history, the results of genetic tests, the use of genetic counseling and other genetic services, and participation in genetic research."[197] Title I of GINA addresses the use of genetic information in the issuance of health insurance, and Title II addresses prohibition of the use of genetic information and confidentiality requirements in employment.[198]

Title I is regulated and enforced by the Department of Labor, the Centers for Medicare and Medicaid Services, and the Department of the Treasury, and it prohibits health insurance companies from asking for, requiring, or using genetic information in assessing eligibility, premiums, coverage, family history, and more.[199] Therefore, it is illegal for a health insurer to use a genetic test result or family health history as a reason to deny coverage, or decide how much someone pays.[200] Title I further prohibits insurance companies from participating in any discriminatory actions, even if the genetic information was inadvertently collected.[201]

Title II, regulated by the EEOC, makes it illegal for employers to use genetic information for hiring or firing purposes, promotions, salary computations, and employment privileges.[202] As all discriminatory practice is prohibited in employment, Title II further bars an employer from requesting, demanding, or purchasing genetic information about a current employee or their family members.[203] Therefore, "it is against the law for your employer to use family health history and genetic test results in making decisions about

197. *Genetic Information*, GENETIC INFO. NONDISCRIMINATION ACT (June 2010), http://ginahelp.org/GINAhelp.pdf.

198. *Genetic Information*, U.S. DEP'T HEALTH & HUM. SERVICES, http://www.hhs.gov/hipaa/for-professionals/special-topics/genetic-information/index.html (last visited Mar. 12, 2016) ("Title I of GINA prohibits discrimination based on genetic information in health coverage. Title II of GINA prohibits discrimination based on genetic information in employment."); *see also Background Information for EEOC Notice of Proposed Rulemaking on Title II of the Genetic Information Nondiscrimination Act of 2008*, U.S. EQUAL EMP. OPPORTUNITY COMMISSION (May 12, 2009), http://www.eeoc.gov/policy/docs/qanda_geneticinfo.html.

199. GENETIC INFO. NONDISCRIMINATION ACT, *supra* note 196 (GINA & Health Insurance section); *see also id.* (GINA & Employment section, How Will GINA Be Enforced subsection).

200. *Id.* (GINA & Health Insurance section).

201. *Id.*; *see also id.* (GINA & Health Insurance section; GINA & My Genetic Services subsection).

202. *Id.* (GINA & Employment section); *see* Genetic Information Nondiscrimination Act of 2008 (GINA) § 203, 42 U.S.C. § 2000ff-1 (2012).

203. GENETIC INFO. NONDISCRIMINATION ACT, *supra* note 196 (GINA & Employment section) ("There are a few exceptions to when an employer can legally have your genetic information. If an employer does have the genetic information of an employee, the employer must keep it confidential and in a separate medical file.").

your employment."[204] Although GINA does protect against the use of genetic information for some purposes, it does not protect against their use for life, disability, or long-term care insurance.[205]

B. GINA Applied to FRT

Although the purpose of GINA is to protect how genetic information is used, the definitions do not seem to apply to FRT used for genetic information. GINA's definition of genetic information encompasses the genetic tests of an individual or his family members and the receipt of genetic services while participating in clinical research.[206] However, genetic information under GINA does not include a person's age or sex, and genetic tests do not include certain analyses completed by a healthcare professional that could reasonably lead to detection of a disease.[207] Under this definition, GINA does not cover FRT as a means of differential diagnosis of genetic conditions. The researchers studying FRT for genetic information are only able to provide likely conditions—not a certain diagnosis.[208] Therefore, this information would not be protected under GINA. Because the software just narrows down a possibility and is not necessarily revealing genetic information, GINA does not clearly apply to such technology. The FRT research on genetic diseases could lead to a loophole in GINA. After all, GINA prohibits employers from requiring or requesting an individual to undergo genetic testing or disclosing the results of a genetic test as a condition of employment.[209] However, it does not prevent an employer from using a photograph of the job candidate to scan through FRT to see the likelihood of a genetic ailment. Therefore, this use must be restricted specifically, either in GINA itself or in the Consumer Privacy Bill of Rights, as discussed in the final Part of this Article.

---

204. *Id.*

205. Mark A. Rothstein, *Currents in Contemporary Ethics: GINA, the ADA, and Genetic Discrimination in Employment*, 36 J.L. MED. & ETHICS 837, 837 (2008).

206. *Id.*; 42 U.S.C. § 2000ff(3)–(4).

207. *See* Rothstein, *supra* note 205, at 838–39 (noting that under GINA, a genetic test "does not include . . . an analysis of proteins or metabolites that is directly related to a manifested disease, disorder, or pathological condition that could reasonably be detected by a health care professional with appropriate training and expertise in the field of medicine involved"); *see also* 42 U.S.C. § 2000ff(7) (defining a genetic test as "an analysis of human DNA, RNA, chromosomes, proteins, or metabolites, that detects genotypes, mutations, or chromosomal changes").

208. *See supra* note 17 and accompanying text.

209. 42 U.S.C. § 2000ff-1(b).

C. HIPAA and FRT For Medical Purposes

HIPAA, in conjunction with its Privacy Rule, "establishes national standards to protect individuals' medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically."[210] Further, in requiring privacy protection for personal health information, it sets limits on the use of the information without individual patient consent and affords rights to patients, such as obtaining copies of their personal health records.[211] HIPAA includes Administrative Simplification provisions, which requires the HHS to implement "national standards for electronic health care transactions and code sets, unique health identifiers, and security."[212] Further, with advances in technology, Congress recognized the need to incorporate provisions that applied federal privacy protection to personally identifiable health information.[213] The HHS furthered the standards governing HIPAA in 2013 with the omnibus rule by expanding the requirements of the HIPAA Privacy and Security Rules to include business associates, such as subcontractors, of the entities that receive protected health information.[214] The Privacy, Security, and Patient Safety Rules of HIPAA are

210. *The HIPAA Privacy Rule*, U.S. DEP'T HEALTH & HUM. SERVICES, http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/ (last visited Mar. 12, 2016); *see also* Health Insurance Portability and Accountability Act of 1996 (HIPAA), 42 U.S.C. § 1320d.

This Article does not address the tort issues that FRT for medical or genetic purposes may bring up. The *Restatement (Second) of Torts*, which has been adopted by a majority of states, enumerates four separate causes of action in the privacy context: (1) intrusion; (2) public disclosure of private facts; (3) false light in the public eye; and (4) appropriation. Shaw, *supra* note 10, at 152–59 (discussing the enumerated privacy torts). An applicable tort that may arise in the FRT context is public disclosure of private facts. This cause of action is defined by the Restatement as "[o]ne who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public." RESTATEMENT (SECOND) OF TORTS § 652D (AM. LAW INST. 1979). Thus, "[this] tort protects people from having facts, even though they are true, published if a reasonable person would be offended at having such intimacies revealed." Shaw, *supra* note 10, at 154.

211. 45 C.F.R. §§ 164.500–.534 (2015).

212. *HIPAA for Professionals,* U.S. DEP'T HEALTH & HUM. SERVICES, http://www.hhs.gov/hipaa/for-professionals/index.html (last visited Mar. 12, 2016); *see also* 45 C.F.R. § 162.1000 (code sets); *id.* § 162.406 (identifiers); *id.* § 162.910 (transactions); *id.* § 164.306 (security).

213. *See generally* 45 C.F.R. §§ 164.500–.534.

214. *New Rule Protects Patient Privacy, Secures Health Information*, U.S. DEP'T HEALTH & HUM. SERVICES (Jan. 17, 2013) [hereinafter *New Rule Protects Patient Privacy*], http://www.hhs.gov/news/press/2013pres/01/20130117b.html.

enforced by the Office of Civil Rights.[215] The final omnibus rule "marks the most sweeping changes to the HIPAA Privacy and Security Rules since they were first implemented," according to HHS Office for Civil Rights Director Leon Rodriguez.[216] "These changes not only greatly enhance a patient's privacy rights and protections, but also strengthen the ability . . . to vigorously enforce the HIPAA privacy and security protections, regardless of whether the information is being held by a health plan, a health care provider, or one of their business associates."[217]

D. HIPAA Applied to FRT

Although there is no direct literature from HHS that states that HIPAA applies to facial recognition technology in conjunction with genetic testing, there are sources that seem to suggest that this is the case. According to an article published in the Journal of Digital Imaging: "Individually identified information, according to [HIPAA], includes 'full-face photographic images and any comparable images.'"[218] A full-facial photograph or equivalent photograph is protected health information (PHI),[219] so a covered entity (most healthcare providers, all health plans, and all healthcare clearinghouses) and business associates would have to comply with the HIPAA use and disclosure requirements when using or disclosing it.[220]

If someone voluntarily provides a photograph to an employer as part of a job application, HIPAA does not apply until it gets in the hands of a covered entity or business associate.[221] Then, HIPAA is triggered and regulates the usage of the photograph. Employment laws, such as ADA and GINA, would regulate this scenario while it is in the hands of the employer.

---

215. *Health Information Privacy*, U.S. DEP'T HEALTH & HUM. SERVICES, http://www.hhs.gov/ocr/privacy/ (last visited Mar. 17, 2016).

216. *New Rule Protects Patient Privacy*, *supra* note 214.

217. *Id.*

218. Jan C. Mazura, Krishna Juluru, Joseph J. Chen, Tara A. Morgan, Majnu John & Eliot L. Siegel, *Facial Recognition Software Success Rates for the Identification of 3D Surface Reconstructed Facial Images: Implications for Patient Privacy and Security*, 25 J. DIGITAL IMAGING 347 (2012), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3348980/. The authors posit that "[i]t remains to be determined whether soft tissue reconstructions of the face have sufficient detail to identify the person to whom such an image belongs." *Id.*

219. 45 C.F.R. § 160.103 (2015).

220. *Id.* §§ 164.500–.514.

221. *Id.* § 164.402.

Also, the language employed in the omnibus rule released in 2013 seems to suggest that genetic information obtained through a facial recognition process would be covered—HIPAA applies to electronic personal health information, and the rule stresses the necessity for privacy maintenance. Additionally, a few companies using FRT in conjunction with genetic testing claim to be HIPAA compliant, thus suggesting that HIPAA should apply to this industry.[222] For example, FDNA[223] alleges compliance with standards set forth through HIPAA and its regulatory agencies by implementation of "the appropriate Security Rule safeguards as part of a corporate commitment to protecting personal data through a strong security and compliance management program."[224] The website individually addresses the security standards set forth and its compliance with each, further demonstrating how HIPAA could be applied to regulate the FRT industry.[225]

One does have a privacy interest in their face, especially if her facial features will be used to see how long she may live or whether she is likely to have a genetic condition.[226] As suggested by the NTIA meetings, a facial template is individually identifiable information.[227] However, if patient consent is obtained or if the personal health information is removed, the medical information would not be covered under HIPAA. Although this information may technically be individually identifiable information, there is no requirement in HIPAA that employers cannot ask for consent to use a facial image of a job applicant or employee. Therefore, although HIPAA may protect the information itself, it does nothing to restrict the use of such information.

E. The FDCA and FRT

This section considers how the FDA may regulate facial recognition software. In addition to its traditional role of regulating food and medicines,

222. *See, e.g.*, FDNA, http://www.fdna.com (last visited Mar. 17, 2016).

223. *HIPAA Compliance Declaration*, FDNA, http://www.fdna.com/hipaa-compliance-declaration/ (last updated Apr. 3, 2014). The FDNA website references Face2Gene, "a genetic search and reference mobile application, powered by the Facial Dysmorphology Novel Analysis technology. Face2Gene facilitates detection of facial dysmorphic features and recognizable patterns of human malformations, while referencing comprehensive and up-to-date genetic information." *Id.*

224. *Id.*

225. *Id.*

226. *See* CTR. FOR DEMOCRACY & TECH., *supra* note 169.

227. *See supra* Part III.F.

the FDA has also regulated medical devices since 1938.[228] More and more, the FDA has sought jurisdiction over computerized medical technology and devices.[229]

Although technology has expanded to a degree where even mobile phones can now be converted into portable medical devices, scholars such as Nathan Cortez argue that the FDA continues to apply an "old regulatory framework to [these] novel products."[230] Cortez describes the current approach of the FDA as overseeing only mobile applications that are medical devices "whose functionality could pose a risk to patient safety if the mobile app were to not function as intended."[231] Cortez critiques this discretionary approach due to the considerably hazy distinction that this draws between products that must be regulated and those that do not.[232] Cortez argues that although the FDA does have jurisdiction to regulate most mobile health technology, the agency may not be equipped to respond to new applications.[233]

The FDA regulates medical "devices" under the federal FDCA.[234] These devices are defined broadly to include "any product intended to diagnose, cure, mitigate, treat, or prevent disease, or any product intended to affect the structure or function of the body."[235] "'Intended use' is a key element in

228. *Regulating Cosmetics, Devices, and Veterinary Medicine After 1938*, U.S. FOOD & DRUG ADMIN., http://www.fda.gov/AboutFDA/WhatWeDo/History/Origin/ucm055137.htm (last updated Dec. 16, 2014); *see also* Nathan Cortez, *Analog Agency in a Digital World* (Working Paper 2014), (on file with author).

229. *See, e.g.*, Ann K. Schooley, *Allowing FDA Regulation of Communications Software Used in Telemedicine: A Potentially Fatal Misdiagnosis?*, 50 FED. COMM. L.J. 731, 743–47 (1998); *see also* Cortez, *supra* note 228.

230. Cortez, *supra* note 228, at 1.

231. Nathan G. Cortez, I. Glenn Cohen & Aaron S. Kesselheim, *FDA Regulation of Mobile Health Technologies*, 4 NEW ENG. J. MED. 371, 374 (2014) (citing FOOD & DRUG ADMIN., MOBILE MEDICAL APPLICATIONS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 7–8 (2013), http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf) ("The FDA cites several examples, including apps that perform electrocardiography or electroencephalography, apps that measure eye movements to diagnose balance disorders, apps that act as wireless remote controls for computed tomography, and apps that control implantable neuromuscular stimulators. The FDA calls these 'mobile medical applications.'").

232. Cortez et al., *supra* note 231, at 374.

233. Nathan Cortez, *The Mobile Health Revolution?*, 47 U.C. DAVIS L. REV. 1173, 1200 (2014). Cortez notes, specifically, that "FDA classifications are not nearly as fluid as software products . . . . Like many new technologies, medical apps can complicate existing regulatory frameworks." *Id.* at 1201.

234. 21 U.S.C. §§ 301–99f (2012).

235. Cortez, *supra* note 233, at 1200–01; *see also* 21 U.S.C. § 321(h) (defining device as "an instrument, apparatus, implement, machine . . . which is . . . intended for use in diagnosis . . . or in the cure, mitigation, treatment, or prevention of disease . . . or intended to affect the structure or any function of

defining 'devices,' and thus in defining the outer bounds of FDA jurisdiction."[236] The agency, by regulation, has defined intended use as the objective intent of how those responsible for marketing the product intend it to be used.[237] The agency can determine objective intent by looking at the product itself, at the manufacturer's claims about it, and at other oral and written statements by those marketing it.[238] Moreover, the FDA can consider the "circumstances surrounding distribution of the article," including widespread consumer use.[239] The FDCA's broad definition of "device" enables the FDA to exercise jurisdiction over computer hardware and software devices.[240] Thus, software that *intends* to perform one of these broad medical functions falls under FDA jurisdiction.[241] Because FDA jurisdiction depends mostly on the way a product functions, the regulated products are wide-ranging and depend upon the presented risks.[242] There are three tiers denoting the authority of the FDA to exercise jurisdiction: (1) "mobile medical apps," which fall within the FDA category of "device" and thus within the jurisdiction of the FDA; (2) applications that fall within the definition of "device" but not within the definition of "mobile medical apps" for which the FDA has discretionary enforcement; and (3) the health applications that do not meet the definition of device and therefore do not fall within FDA jurisdiction.[243] The second

---

the body").

236. Cortez, *supra* note 233, at 1201.

237. 21 C.F.R. § 801.4 (2015) ("The words *intended uses* . . . refer to the objective intent of the persons legally responsible for the labeling of devices. The intent is determined by such persons' expressions or may be shown by labeling claims, advertising matter, or oral or written statements by such persons or their representatives.").

238. *Id.*

239. *Id.*

240. 21 U.S.C. § 321(h); s*ee also* Cortez, *supra* note 233, at 1201–02. The Act defines a "device" as any "instrument, apparatus, implement, machine, contrivance," or similar product "intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease," or any such product "intended to affect the structure or any function of the body." 21 U.S.C. § 321(h). This includes "any component, part or accessory." *Id.*

241. 21 C.F.R. § 801.4. Note, however, that FDA officials testified to Congress that the agency will not rely on actual use to determine "intended use." *See* Letter from Michele Mital, Acting Associate Commissioner for Legislation, Dep't of Health & Human Servs., to Hon. Tim Murphy, Chairman, Subcommittee on Oversight and Investigations, Comm. on Energy and Commerce, House of Representatives 2 (Mar. 20, 2013), http:// www.genomicslawreport.com/wp-content/uploads/2013/03/HousemHealthLetter.pdf.

242. Cortez, *supra* note 233, at 1201 (discussing the three classification tiers and noting that "[t]he higher the classification, the more scrutiny the device receives").

243. BAKUL PATEL, U.S. FOOD & DRUG ADMIN., PUBLIC WORKSHOP—MOBILE MEDICAL APPS DRAFT GUIDANCE 8, 16 (Sept. 12, 2011), http:// www.fda.gov/downloads/MedicalDevices/NewsEvents/

category, wherein the agency exercises discretionary authority, represents the gray area of regulation—compliance for such products may not be required, but is recommended.[244]

The FDA maintains the practice of addressing the regulation of mobile medical apps as they are created.[245] Although the overall approach by the FDA to software is unclear, jurisdiction by the FDA has been exercised on a case-by-case basis.[246] The FDA has created numerous categories encompassing existing products, and many mobile apps may fall within these established classifications.[247] However, the FDA may have to create entirely new categories for the products that do not fit easily within the pre-existing categories.[248] Furthermore, although there are benefits to the case-by-case consideration by the FDA, this approach can be piecemeal and inconsistent if not buttressed with broadly applicable regulations.[249] One concern about the potential FDA regulation of "mobile medical apps" is that many medical applications do not adhere to established medical guidelines.[250] Further, software can be "user-unfriendly" or a user can be vulnerable to "automation

---

WorkshopsConferences/UCM271893.pdf; *see also* U.S. FOOD & DRUG ADMIN., MOBILE MEDICAL APPLICATIONS: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 8, 13 (Feb. 9, 2015), http://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/UCM263366.pdf.

244. Cortez, *supra* note 233, at 1205 ("[T]he FDA says it will regulate apps that obviously are medical devices; . . . it will not regulate apps that obviously are not; and . . . it will defer on the provocative middle tier of apps . . . ."). It is further suggested that "the FDA must be explicit that its guidance documents are not legally binding." *Id.* at 1206.

245. *Id.* at 1209.

246. *Id.* at 1221.

247. Nathan Cortez, *Regulating Disruptive Innovation*, 29 BERKELEY TECH. L.J. 175, 193 (2014). This includes: "medical calculators, cameras, lights, magnifiers, microscopes, monitors, recorders, reminders, scales, surgical tools, transmitters, and a host of data systems that store, display, and manipulate information." *Id.* at 193 n.96.

248. Cortez, *supra* note 233, at 1221–22 ("But many [devices] will fit uneasily, or not at all. And in such cases, the FDA might have to create entirely new categories . . . .").

249. Cortez, *supra* note 247, at 193 ("The agency did pre-clear discrete software products on a case-by-case basis, which could serve as precedent for similar products. But this piecemeal approach fell far short of establishing a definitive, cohesive philosophy towards software that companies could use to predict their regulatory obligations.").

250. Cortez, *supra* note 233, at 1193 (providing as an example a case study of smoking cessation apps, very few of which conformed to "the evidence-based clinical practice guidelines for smoking cessation programs"); *accord* Rochelle Sharpe, *Lacking Regulation, Many Medical Apps Questionable at Best*, NEW ENG. CTR. FOR INVESTIGATIVE REPORTING (Nov. 18, 2012), http://necir.org/2012/11/18/medical-apps/ (noting that few health and wellness apps "follow established medical guidelines, and few have been tested through . . . clinical research").

bias."[251] Additionally, the "piecemeal and sporadic" regulation by the FDA is potentially problematic because of both the case-by-case review by the agency and reliance on non-binding guidance.[252] Many scholars believe that the FDA still lacks the resources to adequately regulate the influx of software devices and that "as software devices become more ubiquitous and critical to patient care, the FDA's regulatory framework remains inert."[253] An example of the influx of software is mobile health applications. As of March 2013, there were approximately 97,000 different applications, hundreds to thousands that qualify as medical "devices."[254] Another worry is that the software industry is not prepared to comply with the "technical FDA requirements," and the FDA consistently applies a "least burdensome" approach to software regulation.[255]

F. FRT and the FDA

Mobile health applications used on smartphones and tablets may function as medical devices, allowing for "customized diagnoses and treatment recommendations by comparing user-specific data to vast bodies of clinical research and accumulated medical knowledge."[256] Similarly, FRT is based on systems and computer programs that analyze images for identification purposes.[257] As previously discussed, FRT is being used for a myriad of purposes, including predicting lifespans.[258] Furthermore, there are upwards of 17,000 genetic disorders that have been diagnosed, of which about 700 can be diagnosed with the assistance of abnormal facial characteristic recognition.[259] Currently, FRT correctly predicts a genetic disorder, on average, 93% of the time.[260] It is important to protect "biometric information from exploitation and misuse," and government intervention and statutory legal protection may be helpful with this.[261] The FDA may be an appropriate platform to initiate such

251. Cortez, *supra* note 228, at 5. Automation bias refers to "the belief that automated computer processes are infallible or simply less prone to make errors than they actually are." *Id.*
252. *Id.* at 6.
253. *Id.* at 7.
254. *Id.* at 10.
255. *Id.* at 12.
256. Cortez, *supra* note 233, at 1177.
257. *Q&A on Face-Recognition*, *supra* note 6.
258. Klimas, *supra* note 85.
259. Clark, *supra* note 15.
260. Weller, *supra* note 1.
261. NAT'L TELECOMM. & INFO. ADMIN., AN ETHICAL FRAMEWORK FOR FACIAL RECOGNITION 2,

regulation, intervention, and legal protection. Within the FDA's case-by-case approach under the second tier of its analysis, FRT would fall under discretionary approval by the FDA as its uses can be classified as "devices" within the applicable analysis. This may not be the ideal platform because the current uses of FRT in the medical context do not necessarily fall within "mobile medical applications." As FRT software develops more in the medical context, the FDA may be a logical step in the regulation of this technology. However, as currently structured, there is not clear protection of consumers and patients via the FDCA.

G. ADA and FRT for Medical Purposes

Another law that may help protect patients and employees from discrimination based on FRT software is the ADA, which prohibits discrimination on the basis of disability.[262] The ADA's definition of "an individual with a disability" is one whose "physical or mental impairment that substantially limits one or more major life activities of such individual; a record of such an impairment; or being regarded as having such an impairment."[263] Prior to the ADA Amendments Act of 2008 (ADAAA), the EEOC had issued a non-binding interpretation in 1995 stating that individuals who are discriminated against on the basis of "genetic information relating to illness, disease, or other disorders," are protected by the ADA.[264] However, the ADAAA superceded this guidance and did not seem to clarify if the ADA would cover the position of the EEOC.

Under the ADA, a disability is defined as "a physical or mental impairment that substantially limits one or more major life activities of such individual; a record of such an impairment; or being regarded as having such an impairment."[265] The ADA does not specifically list all of the various disabilities that are covered under the Act.[266] However, the broad definition contained within the ADA expressly excludes only "transitory and minor"

---

https://www.ntia.doc.gov/files/ntia/publications/aclu_an_ethical_framework_for_face_recognition.pdf (last visited Mar. 17, 2016).

262. 42 U.S.C. § 12101(b) (2012).

263. *Id.* § 12102(1)–(3).

264. *EEOC Compliance Manual*, vol. 2, EEOC Order 915.002, 902–45.

265. 42 U.S.C. § 12102(1); *accord A Guide to Disability Rights Laws*, U.S. DEP'T JUST. (July 2009), http://www.ada.gov/cguide.htm.

266. *A Guide to Disability Rights Laws*, *supra* note 265.

impairments.[267] Therefore, the statute likely protects hidden disabilities, or "impairment[s] causing limitations not obvious to the naked eye, not easily discerned by others, or not noticeable in the person's speech, behavior, or mobility." including impairments that may have an effect on the "brain, circulation, respiration, muscular or skeletal system, sensory abilities, etc."[268]

There are several stereotypes associated with hidden disabilities, including that "hidden disabilities are not believable, [they are] not as severe as obvious disabilities like mobility impairments, [they] are hard to accommodate because the need is not obvious, and people with hidden disabilities do not need accommodations."[269] Thus, disclosure of a hidden disability in the workplace can be a difficult decision for an employee to make.[270] "If you announce your condition, you risk being stigmatized; if you keep it a secret, you risk poor performance reviews or even being fired."[271] Therefore, benefits of nondisclosure—including maintenance of privacy and confidentiality in the workplace, as well as avoiding stigmatization—could be said to outweigh those of disclosure.[272]

H. ADA Applied to FRT

It is unlikely that an unexpressed genetic condition or likelihood would rise to the definition of disability. Also, a short predicted lifespan would also not be deemed a disability under the ADA. Those with a potential genetic predisposition to future illness are likely not covered by the ADA.

---

267. 42 U.S.C. § 12102(3).

268. SUZANNE R. GOZDEN, U.S. DEP'T LABOR, TO DISCLOSE OR NOT TO DISCLOSE 5, http://accessibilityonline.s3.amazonaws.com/archives/2004-06-15%5EDisclosure.pdf (last visited Mar. 17, 2016). This category would include impairments that may have an effect on the "brain, circulation, respiration, muscular or skeletal systems, sensory abilities, etc." *Id.* Listed examples include: epilepsy, ADD, sleep disorders, migraines, fibromyalgia, depression, PTSD, learning disabilities, HIV/AIDS, cancer, diabetes, heart conditions, respiratory impairments, vision loss, and hearing loss. *Id. Contra* Lawrence D. Rosenthal, *Can't Stomach the Americans with Disabilities Act? How the Federal Courts Have Gutted Disability Discrimination Legislation in Cases Involving Individuals with Gastrointestinal Disorders and Other Hidden Illnesses*, 53 CATH. U. L. REV. 449, 449 (2004) ("[I]t has become clear that many people who have 'hidden' illnesses are not benefitting [from the ADA].").

269. GOZDEN, *supra* note 268, at 6.

270. Katherine Bouton, *Quandary of Hidden Disabilities: Conceal or Reveal?*, N.Y. TIMES (Sept. 21, 2013), http://www.nytimes.com/2013/09/22/business/quandary-of-hidden-disabilities-conceal-or-reveal.html.

271. *Id.*

272. GOZDEN, *supra* note 268, at 7–8.

VI. RECOMMENDATIONS: PROPOSED RESTRICTIONS ON THE USE OF FRT FOR MEDICAL AND HEALTH PURPOSES

The analysis in Part IV of this Article makes clear that the health privacy, genetic, FDA, and disability laws in the country do not protect the use of FRT by employers or insurers for their own discriminatory purposes. There is currently no federally applicable law that specifically addresses FRT, although some states have passed legislation attempting to address the issues.[273] The lack of legislation raises concerns including the possibility of privacy violations, freedom of speech restraints, and stalking.[274] Although the American population acquiesces to governmental monitoring for security purposes, people still expect a certain amount of privacy in their daily lives.[275] Both the "government and the private sector have the capacity for surveillance of nearly everyone in America."[276] There is no current constitutional basis to prevent this, and no constitutional text that "plac[es] boundaries on the government's ability to engage in ubiquitous monitoring of citizens based on images snapped in public or posted online."[277] Therefore, there is no constitutional control covering corporations and individuals for generating the databases of personal information, and there is no cap on governmental power in obtaining it.[278]

Another concern noted is that although this technology can be helpful in the context of criminal law and the use by law enforcement, it "can also perpetuate racial and ethnic profiling, social stigma, and inaccuracies throughout all systems and can allow for government tracking and surveillance on a level not before possible."[279] Furthermore, "[u]sing facial recognition technology beyond checking attendance or to maintain security could be a

273. Kirill Levashov, Note, *The Rise of a New Type of Surveillance for Which the Law Wasn't Ready*, 15 COLUM. SCI. & TECH. L. REV. 164, 176–77 (2013).

274. *Id.* at 187.

275. Brown, *supra* note 10, at 409 ("[P]eople also expect to go about daily life in relative obscurity—unidentifiable to others they do not already know, do not care to know, or are not required to know—so long as they abide by the law.").

276. *Id.*

277. *Id.* at 410 ("The Supreme Court has made clear that the Fourth Amendment does not protect '[w]hat a person knowingly exposes to the public.' Nor does it cover information revealed to third parties.").

278. *Id.*

279. Kathy Gurchiek, *Facial Recognition Technology Raises Privacy Issues*, SOC'Y FOR HUM. RESOURCE MGMT. (Sept. 14, 2012), http://www.shrm.org/hrdisciplines/technology/articles/pages/facial-recognition-privacy.aspx.

slippery slope into privacy issues if its use by employers or their vendors veers into sourcing potential job candidates."[280] The counter-argument is that FRT will be so expensive to implement that it is not likely that it will be used in the employment context.[281] However, FRT, like any new technology, will be cheaper as it becomes more ubiquitous.[282]

Restrictions are needed to prevent employers, insurers, and any other entity or individual from using FRT for medical or health purposes without the individual's specific consent. Furthermore, employers and insurers should be restricted from being able to ask for this information—or for any genetic information. Such a restriction will protect individuals from feeling coerced into consenting. There are definite upsides to the FRT research described in this Article. However, it is necessary to protect individuals from unwittingly revealing medical and health information.

The most direct fix to the issue of the misuse of FRT for medical purposes would be the enactment of a regulation interpreting GINA that makes clear that FRT cannot be used by employers or insurers for the purpose of attempting to determine genetic predispositions. This would be the clearest way to ensure that GINA works as it is intended to. Including tests or software that narrows down a possibility of genetic predispositions in the definition of genetic information in GINA would close the loophole in GINA discussed earlier.

Additionally, the Consumer Privacy Bill of Rights may be amended to address the medical and health potential of FRT. The July 2014 NTIA meeting considered the Consumer Privacy Bill of Rights.[283] Specifically, the stakeholders discussed: (1) what type of entities the code provisions would apply to; (2) obligations imposed when no "facial template" is created; (3) what obligations are imposed when the information is not stored; (4) the risk of individual's information being stored without consent or knowledge; (5) the worry that a code of conduct "could preclude or hinder meritorious uses of commercial FRT"; (6) individuals being denied product or services based on a

280. *Id.*

281. *Id.* (noting that at least some experts in the field "think[] the cost of the technology will be so prohibitive that many employers will not use it.").

282. Matt Rosoff, *Every Type of Technology Has Gotten Cheaper over the Last Two Decades—Except for One*, BUS. INSIDER (Oct. 14, 2015), http://www.businessinsider.com/historical-price-trends-for-tech-products-2015-10 ("As technology gets more advanced, prices drop and products get better.").

283. *Privacy Multistakeholder Process: Facial Recognition Technology*, *supra* note 181; *see also NTIA Seeks Comment on Big Data and the Consumer Privacy Bill of Rights*, NAT'L TELECOMM. & INFO. ADMIN. (June 4, 2014), https://www.ntia.doc.gov/press-release/2014/ntia-seeks-comment-big-data-and-consumer-privacy-bill-rights.

refusal to consent to enrollment of a facial recognition template; (7) risk of commercial use of FRT infringing on personal autonomy and erosion of personal privacy; (8) the chilling effects on free speech and free assembly; (9) risk of unanticipated commercial use of the technology that consumers do not understand; and (10) the risk that FRT could result in discriminatory practices or patterns of behavior such as predatory marketing.[284] Each of these ten concerns is important, but does not address what kind of regulatory mechanism is needed for FRT for medical and health purposes. Even if a facial template is not stored, it is necessary to have privacy protections when FRT can reveal private health information. The Consumer Privacy Bill of Rights could be a good way to ensure privacy, but it needs to be expanded to include issues that are central to medical or health information, as suggested above.

FRT software is developing rapidly to address a whole host of health-related issues. The law must catch up to this technology. The answer is not necessarily to prevent the development of this technology—but rather to ensure that the way it is used is consistent with the laws that protect genetic privacy.

284. NAT'L TELECOMM. & INFO. ADMIN., NTIA MULTISTAKEHOLDER PROCESS ON FACIAL RECOGNITION TECHNOLOGY 1–4 (2014), https://www.ntia.doc.gov/files/ntia/publications/ntia_draft_list_of_issues_7_22_14.pdf.

***

***

***